THE ILLUSION OF PRIVACY:

ASSESSING THE USE OF BIG DATA FOR AD TARGETING ON SOCIAL MEDIA

Nicole Danielle Lang

TC660H

Plan II Honors Program

The University of Texas at Austin

May 11, 2017

Kathrynn Pounders, Ph.D.

Stan Richards School of Advertising & Public Relations

Supervising Professor

Lucy Atkinson, Ph.D.

Stan Richards School of Advertising & Public Relations

Second Reader

Abstract

Author: Nicole Danielle Lang

Title: The Illusion of Privacy: Assessing the Use of Big Data for Ad Targeting on Social Media

Supervising Professor: Kathrynn Pounders, Ph.D.

For modern-day advertisers, data is everything. This paper explores how data is used in paid social media advertising and examines the fine line between ad relevancy and a breach in privacy. Additionally, this thesis assesses the ethical responsibility of data brokers, social media platforms, U.S. government, and consumers for upholding user privacy. After researching current legislation and reviewing privacy policies, this thesis finds there is an insufficient amount of regulation. Additionally, interviews included in this study discovered a general unawareness of how data is being collected and sold by social media platforms.

Acknowledgements

This thesis would not have been finished without the love and support of so many. To everyone involved, thank you for your encouraging words and for your genuine interest in my project.

A special thank you to my parents and sister. Mom, thank you for your unconditional support, for hours of editing, and for flying back early just to see my eight-minute presentation. Dad, thank you for always taking the time to ask about my progress and reminding me to finish strong. Kali, thanks for being my big sister, my role model, and my extra set of eyes.

Friends, roommates, and extended family, thank you for listening me talk nonstop about my ad targeting. Seeing your interest in my topic kept me excited about the research. I hope I did not make y'all too paranoid about online privacy! To Gabby, you have helped me in more ways than you know. Since our initial thesis brainstorm in Switzerland, you are the first person I turn to for a question or advice. To Eleni, thank you for eleven years of school and for countless hours at Austin coffee shops. There is no one else I would rather partially work and partially get distracted with.

Finally, my deepest thank you to my advisors Dr. Kathrynn Pounders and Dr. Lucy Atkinson. Thank you for agreeing to supervisor this project when I still had a million ideas in my head. Both of you kept me on task throughout the year and kept my morale high. When I was anxious or overwhelmed, you both assured me everything would work out. It has been a pleasure to work with the two of you.

Table of Contents

Chapter 1: Introduction

If you think advertising is dead, you do not know anything about advertising. In correlation with the digital age, advertising has evolved into a complex, segmented industry. Ads are no longer limited to rigid thirty-second television spots and black and white newspaper ads; ads can be seen everywhere, i.e. in music videos, on bikes, and your very own smartphone. In numerous situations, the line between advertising and personal content is blurred with the influx of native content and brand partnerships with social influencers. Amongst all these changes, however, I would argue the greatest change has spurred from the advertising industry's newfound reliance on data. Data drives decisions because it allows brands to optimize and track success in real time. Brands save money through data by serving hyper-specific ads to selected individuals at specific times. Data removes many uncertainties by directly addressing the success and impact of a campaign. While data is an invaluable tool for brands, at what cost does it come to the consumer? This is the driving question behind this thesis.

Specifically, this thesis examines and assesses how brands target consumers through paid social media. Paid social media refers to all forms of advertising where brands pay for ad placements. The focus of this project is on advertising placed through three social platforms: Facebook, Snapchat, LinkedIn. These platforms were selected because they each serve a different communicative purpose. The platforms have different core age demographics and have varying relationships with advertisers. Social media is a media and ad platform that rapidly updates, changes, and restructures. Therefore, there is a lack of extensive academic related research. However, this project pulled from related topics such as Big Data, anonymization, and user privacy. This thesis attempts to compile and consolidate relevant ad policies and various attempts

at regulating data usage. This includes careful examination of each platform's current privacy policies by tracking shifts in policy overtime. By outlining policies, or lack thereof, this project identifies ways in which data can exploit an individual's privacy.

Another question this thesis answers is whether consumers are aware and/or comfortable with the personal data being collected and shared on them. Anecdotal responses were collected and analyzed after eight in-depth interviews with female consumers. Participants shared their opinions on data, privacy, and ad targeting. Individuals also shared what interest groups Facebook categorized them, based on the site's Ad Preference feature. These interviews exposed a shared misunderstanding of how their data was being used and shared. In terms of law, individuals believed there were more protections and regulations than currently in place. Lastly, these interviews demonstrated the inefficiencies of social platform's privacy policies for educating users on data sharing and online privacy.

The questions answered and topics covered by this thesis are questions every advertiser and brand should ask. Big Data is a great tool, but every advertiser needs to understand the implications of using certain sets of data. By taking into consideration how Big Data can be the potential root of discrimination or bias, we can hopefully keep Big Data as something more helpful than harmful. When thinking about data's role in advertising, a Spiderman quote sums it up best, "With great power, comes great responsibility." Data is a powerful tool because it allows brands to make inferences based on users actions and behavior. It also requires responsibility so that data is not used as a weapon for inequality and harm.

Chapter 2: Targeted Advertising

Advertising is more than communication between brands and consumers; it represents the ever-present advances in technology. While new technologies shift how an advertisement is delivered, the core tenets of effective advertising remain the same. Advertisements must be relevant, be personal, be creative, and be present. If an advertiser can deliver the right message at the right time to the right audience, they have achieved their goal. One process by which brands reach this goal is through ad targeting. Ad targeting is generally defined as the "automated and specific alignment of any advertising media according to different parameters. It enables the optimized delivery of digital advertising at defined audiences i.e. target groups minimizing losses due to waste coverage" (Schlee, 2013). Ad targeting optimizes a brand's advertising campaign and ensures spending is done efficiently.

The original intent of targeted advertising was to minimize media spend on non-users, users who do not and will not use that brand. Today, the influx of consumer information has repurposed targeting from simply avoiding non-users to actively pursuing specific buyer segments. Researchers attribute this change to two key shifts in the market environment. First, brands have more access to consumer information, such as their preferences and their media habits. With this information, brands can deliver the right message through hyper-specialized ads. Second, a rapid expansion of new advertising media platforms has provided brands the ability to target specific segments within a market (Iyer, Summer 2005). Whereas, brands that used to only buy broad, thirty-second television spots on network television, now purchase ad space on sites with specific articles, messaging, and content. Through these efforts, there is more focus on the individual rather than a group.

Defining Targeting Tactics

Targeted advertising is a practice in which brands serve ads dependent on the receptiveness of different audiences. One common practice advertisers use is building out detailed, consumer profiles. Brands look at their current consumer base and identify common behaviors or demographics. These characteristics are added to a consumer profile. From this, brands can identify other potential customers to target. Consumer profiles allow brands to target individuals who express similar characteristics, without having to identify the identity of different individuals. In theory, these profiles protect an individual's private online information and consumers purchasing patterns.

Advertisers and brands target these profiles through a diverse set of tactics. Differentiating these tactics is essential for understanding the complex opportunities for consumer targeting. These tactics are not media specific (i.e. television and radio) but their roles change dependent on the media (Schlee, 2013). In general, digital media allows for greater target precision than traditional mediums. Although targeting reduces the reach of a campaign, it increases the relevancy and often leads to higher success rates. Below are definitions and examples for seven commonly used forms of ad targeting:

Contextual Targeting

Contextual targeting is the most basic form of targeting, where brands buy ads based on a medium's content. This form of targeting is based on the genre of a radio station, demographics of a television show, or type of articles on a website. A simple example of contextual targeting is Speedo Swimwear placing a digital ad next to an article about Olympic swimming.

Time Targeting

The second most common form of targeting is time targeting, also known as day parting. Time targeting is a form that uses time as a qualifier for serving ads. By selecting the time of day an ad is served, brands hope to increase relevancy dependent on their product or service. For example, it would be beneficial for a breakfast-only restaurant to spend ad dollars during their morning hours of operation and not late in the evening. Advertisers use time targeting as a tool to protect them against ad fraud, the second largest crime worldwide (Vranica 2014). Ad fraud is when cyber criminals charge advertisers for ads never run, not viewable, or served on fake websites. Peak hours for ad fraud is between 1AM and 5AM. Knowing this, some brands block their ads from running during this time.

Socio-demographic Targeting

Socio-demographic targeting focuses on characteristics of a consumer including age, gender, salary, and nationality. When creating consumer profiles, this tactic quickly narrows down large sums of people. Some brands are even required by law to factor out certain socio-demographic groups based on the associated content. For example, cigarettes, alcohol, and weapons are all products that cannot target minors due to law. Another use of socio-demographic targeting is for gender related products, i.e. Tampax only markets feminine products towards female consumers.

Geographic Targeting

Geographic targeting is targeting based on location. Technology has enabled geographic targeting in real time. Today, brands can send ads to consumers based on their current location. For example, Gap clothing stores use geo-fencing to serve super localized ads that are only displayed when consumers are within a certain radius (Ha, 2012). Brands also use geographic

targeting to reach ZIP codes with a common demographic or regions with a special need for a product. This is why Texans do not regularly receive ads for snow boots or New Yorkers for cowboy boots.

Technical Targeting

Technical targeting is when brands target consumers based on their hardware or software status. Nike, for example, might only serve video ads to a consumer if they have a strong Internet connection. This ensures ad dollars are not wasted on consumers that cannot see the full advertisement.

Behavioral Targeting

Behavioral targeting has rapidly expanded with the rise of online shopping and its associated data. It is "the practice of collecting data about an individual's online activities for use in selecting which advertisement to display" (McDonald 2010). Brands create "profiles for Internet users based on a variety of different data types and inferences [...] Third-party cookies are one of several mechanisms used to enable behavioral advertising [...] noting every time a given user visits any of the sites in the network." Through cookies and trackers, brands collect immense knowledge on their consumer and their preferences. "By correlating which sites an individual visits, ads clicked, inferences about age range and sex, and approximate physical location based on the computer's IP address, advertisers build profiles of that individual's characteristics and likely interests" (McDonald and Cranor 2010). Unlike other forms of targeting, behavioral advertising is based on inferences. Brands use data to make connections between online behaviors and potential customers. For example, Anthropologie might track and flag customers who visit their site and use a 20% off coupon code. Moving forward, these customers will

receive more promotion-based ads instead of generic ones based on their behavioral history of responding to coupons.

Retargeting

Finally, retargeting is the most discernable form of targeting. Retargeting occurs when a consumer visits a site, views or adds an item to her basket, and then leaves the site without making the purchase. With tracking and cookies, the brand can then retarget the consumer through an ad that showcases the exact product previously considered for purchase. How many times have you looked at a pair of shoes on Nordstrom's website, and then seen those exact shoes while scrolling through your Newsfeed on Facebook? This is a prime case of retargeting.

Chapter 3: Paid Social

Paid social includes all paid advertisements on social media platforms. With brands spending sixty-five percent more of their ad spend on Facebook, Twitter, LinkedIn, Instagram, and Pinterest in 2016 than in 2015, this medium is quickly growing (Handley 2016). Unlike traditional media that require large budgets and extensive planning, paid social is accessible to small companies with low budget. Paid social is a rewarding medium because advertisers can monitor and optimize results in real-time. In addition, brands can engage in hyper-specific targeting to reach specific audiences. This thesis focuses on three diverse social media platforms: Facebook, Snapchat, and LinkedIn. Instagram is also referenced throughout this study, since Facebook owns and operates Instagram's advertising dashboard.

Facebook

Facebook is currently the largest social media network and platform in the United States. Founded by Mark Zuckerberg in 2004, Facebook currently has 1.94 billion monthly active users worldwide (Facebook 2017). The first form of advertising on Facebook was through standard banner ads by J.P. Morgan Chase in August 2006 (Kessler 2011). Since then, advertising on Facebook has relied heavily on advances in technology and data.

Privacy Policy

Before ads shows up on Facebook or Instagram, Facebook must approve the advertisement by checking that the ad complies with Facebook's Advertising Policies. The reason behind this vetting process is to protect users from offensive messaging and online scams. To date, Facebook has 5 types of restricted content and 25 types of prohibited content for advertisers. The 5 types of

restricted content are alcohol, dating, real money gambling, state lotteries, and supplements. The 25 types of prohibited content range from illegal products, adult content, weapons, false content, profanity, and personal attributes. To clarify what no personal attributes entails, Facebook Advertising Policies states:

> "Ads must not contain content that asserts or implies personal attributes. This includes direct or indirect assertions or implications about a person's race, ethnic origin, religion, beliefs, age, sexual orientation or practices, gender identity, disability, medical condition (including physical or mental health), financial status, membership in a trade union, criminal record, or name."

Facebook further claims they "do not use sensitive personal data for ad targeting. Topics [advertisers] choose for targeting [their] ad don't reflect the personal beliefs, characteristics or values of users" (Facebook 2016). While this policy appears straightforward, in reality, Facebook's Advertising Policies are complex, deceiving, and riddled with loopholes.

As expected, brands have found ways around prohibited content through strategic targeting, and Facebook is partly to blame. On Facebook's policy page, there are examples of what to and not to include in an ad, which gives creative direction to advertisers. For example, an advertisement can say "meet black men today" but not "find other black singles" (Facebook 2016). Similarly, an advertisement can say, "meet Christian women" but not ask, "Are you Christian?" (Facebook 2016) With these slight differentiators, Facebook distinguishes these ads as being more ethical, but it is unclear whether this is true. At the end of the day, individuals are still targeted based on certain qualifications but are approached in a more subtle way, because Facebook does not want its users to be fully aware of the targeting practices that take place.

Facebook specifically addresses target advertising with two main rules. The first rule states, "You must not use targeting options to discriminate against, harass, provoke, or disparage users

or to engage in predatory advertising practices" (Facebook 2016). Second, "If you target your ads to custom audiences, you must comply with the applicable terms when creating an audience" (Facebook 2016). These custom audiences, referred to by Facebook as "hashed data," are created through a Facebook feature that enable brands to create an audience using brand-obtained data such as email addresses or phone numbers. Brands can then combine their first-party data with second and third party data, purchased from Facebook. The more data a brand obtains, the more highly targeted their ads will become.

Ad Preferences on Facebook are based on site activity. "The ads you see are influenced by a variety of factors, the most basic of which is the demographic information—such as age, gender and location—from your profile and activity" (Facebook, 2016). Facebook, however, is not fully transparent with all of the intricacies behind this process. While Facebook claims ad preferences optimizes its user' experience, ProPublica suggest ad preferences monetize off user experiences (ProPublica, 2016). Different organizations have started pressuring Facebook to be more transparent regarding its ad platform. This comes after several ethical concerns regarding Facebook's ad targeting.

Political Views

Facebook categorizes and labels all of its users based on their site activity. ProPublica found that there are "nearly 50,000 unique categories in which Facebook places it users" (ProPublica 2016). One labeled characteristic is a user's political views. Advertisers and politicians were able to use this information during the 2016 election by serving ads only to liberals, moderates, or conservatives. The primary concern with political labeling is that Facebook labels individuals based on their activity on the site and not necessarily users' true political views. A New York

Times article explained, "Even if [a user does] not like any candidates' pages, if most of the people who like the same pages— such as Ben and Jerry's ice cream — identify as liberal, then Facebook might classify [that user] as one, too" (Merill 2016). Through micro targeting, "finding and combining information about individuals' political preferences and consumer habits" (Kruikemeier 2016, 367), political parties can deliver messaging that resonates with Facebook users. "Facebook's micro targeting is particularly helpful for advertisers looking to reach niche audiences, such as swing-state voters concerned about climate change" (Angwin and Parris 2016). Facebook uses self-collected data to make generalizations about its users' without majority awareness.

Campaigns find these capabilities invaluable because it reduces wasted media spend and allows for diversified messaging. The Trump and Clinton campaign sent unique messages amongst its varying voter groups and levels of supporters. For example, "Donald J. Trump's presidential campaign [...] paid for its ads to be shown to those who Facebook has labeled politically moderate" (Merill 2016). Trump had a better chance persuading a political moderate than targeting a user who Facebook categorizes as politically liberal. Similarly, the Clinton campaign ran ads to look-alike audiences. Look-alike audiences are users whose Facebook activities, likes, demographics, and clicks, resembled people who already liked Clinton's Facebook page. Through this feature, "the candidate does not directly get a list of names, but the Clinton campaign […] runs ads to "look-alikes" asking them for their email addresses so that [the campaign] can directly reach [targeted Facebook users] via email later" (Merill, 2016). While each candidate took a different targeting approach, both relied heavily on Facebook advertising to recruit voters and raise funds.

The Political Ad Track Project, conducted by The New York Times, asked readers to submit political ads they saw on Facebook throughout the 2016 election (New York Times, 2016). One submission was an ad to "vote early in Florida." So, a user viewed the ad and discovered "This ad was targeted to an adult who lived in Florida, a battleground state, and who was part of an audience it called "Ethnic affinity — African American (US)" (Merill 2016). This is a clear example of how Facebook's labeling directly led to a political ad being served.

While ad targeting increased each campaign's relevancy, it also contributed to a general unawareness about the alternative party. Since voters on either extreme were only served ads for their specific party, they were not given the opportunity to understand both candidates' platforms and messaging. Here is one reason why Democrats were shocked by November's results. Liberals on Facebook were only being served ads for Hilary Clinton and were largely unaware of the heavy and effective marketing efforts by the Trump campaign.

Ethnicities

In regards to race and advertising, Facebook has had a troubled past. Its advertising policies clearly state that serving ads dependent on race is strictly prohibited. However, on October 28, 2016, ProPublica exposed a loophole in which advertisers were able to discriminate through ads based on race. They proved this by running a real ad in Facebook housing categories. The ad they purchased "was targeted to Facebook members who were house hunting and excluded anyone with an "affinity" for African-American, Asian-American or Hispanic people" (Angwin and Parris 2016). By adding this affinity filer, ProPublica successfully discriminated against minority races.

This capability is inconsistent with The Fair Housing Act of 1968 and The Civil Rights Act of 1964, acts that make it illegal to discriminate on the bases of race. When ProPublica first filed its complaint to Facebook, Privacy and Public Policy Manager Steve Satterfield replied saying, "We take a strong stand against advertisers misusing our platform: Our policies prohibit using our targeting options to discriminate, and they require compliance with the law" (ProPublica 2016). However, he believed this function was important for advertisers wanting to test marketing strategies and languages across various affinity groups. Satterfield continued, "Facebook began offering the 'Ethnic Affinity' categories within the past two years as part of a 'multicultural advertising' effort" (ProPublica 2016). Essentially, "Ethnic Affinity" is not the same as race to Satterfield. ProPublica published an article detailing this interaction, which Facebook immediately responded to through a blog post by Christian Martinez, Facebook's Head of Multicultural at Facebook. Martinez wrote, "Everyone benefits from access to content that's more relevant to them. But this is especially critical for people who choose to affiliate with ethnic communities" (Martinez, 2016). Martinez showed no indication that Facebook's actions were immoral or illegal, finishing the post with:

> "To do this, we can't pretend that diversity doesn't exist, or ask diverse communities to resign themselves to seeing only ads whose very existence calls them out as different. Instead, we need to enable everyone to see the content that's most relevant to them — and work to encourage everyone to embrace, not suppress, the diversity that makes our community great."

Due to public backlash, this original sentiment was short lived. On November 11, 2016, several weeks later, Facebook decided to stop some of its ethnic-affinity targeting. Facebook's US Public Policy and Chief Privacy Officer, Erin Egan, announced this change through a blog post. She wrote, "there are many nondiscriminatory uses of our ethnic affinity solution in these areas, but we have decided that we can best guard against discrimination by suspending these types of

ads" (Egan 2016). While advertisers can still use ethnic-affinity to target groups, Facebook promised to create tools that block ads that use ethnic-affinities to discriminate on "housing, employment and the extension of credit" (Egin, 2016). In addition to removing these tools, Facebook promised to "update [its] Advertising Policies to be even more explicit and require advertisers to affirm that they will not engage in discriminatory advertising on Facebook, and [Facebook] will offer new educational materials" (Facebook 2016). The post also noted that Facebook is working with "New York State Attorney General Eric Schneiderman, US Rep. Robin Kelly of Illinois and the Congressional Black Caucus, and US Rep. Linda Sánchez of California and the Congressional Hispanic Caucus," to update ethnic-affinity marketing. This is a key detail because it acknowledges that legal entities, policy-makers, and civil rights activist had not played a major role in Facebook's targeting prior to the investigation.

Here, Facebook's change in policy directly resulted from public criticism. Had ProPublica not investigated Facebook's affinity targeting, other brands might have secretly utilized the same filter for discrimination. While ProPublica's actions benefited minority groups, it raises concerns on why Facebook's targeting methods had not been regulated, monitored, or audited by a third-party service beforehand.

Facebook Ad Preferences

Beyond changes in ad policy, Facebook allows every user an opportunity to edit and remove any labels attributed by Facebook. By following "https://www.facebook.com/ads/preferences," users are redirected to a personalized Ad Preferences page. Here, users learn what influences the ads they see and have the chance to "take control of their ad experience" (Facebook 2016). The main

section on this page is labeled “Your interests.” In your interests, there are fourteen different categories that users can look through. These include: news and entertainment, business and industry, travel places and events, hobbies and activities, people, food and drink, sports and outdoors, shopping and fashion, technology, education, lifestyle and culture, fitness and wellness, family and relationships, and other. In each category, there is a list of brands, topics, and interest that Facebook believes are relevant to the user. Once the interest is clicked on, Facebook shows examples of related ads. Depending on whether the interest is relevant, a user can click “not interested” which removes specific brand targeting moving forward.

Other sections included in Ad Preferences are: advertisers you’ve interacted with, your information, ad settings, and how Facebook ads work. “Advertisers you’ve interacted with,” enables users to see which brands have their contact information, which website or apps they’ve used, and whose ads they’ve clicked. The last feature is important for users to quantify how often they interact with advertisements on Facebook. In the “Your Information” section, users can manage whether Facebook can show ads based on different types of disclosed information. This section is less about behavioral targeting and more about demographic and technical targeting. In the “Ad Setting” section, one particular setting stands out. Facebook asks users “Can your Facebook ad preferences be used to show you ads on apps and websites off of the Facebook Companies” (Facebook 2017). The default setting is set to yes. While this setting is hidden under Facebook Ad Preferences, it gives Facebook the legal right to sell its users information for practices beyond its social platform. Facebook sells this information through The Facebook Audience Network.

As of December 2016, Facebook is testing a new ad feature: Hide ad topics. The platform is testing this feature by giving users an opportunity to limit advertisements regarding sensitive topics for six months, one year, or permanently. Currently, this feature is only applicable to alcohol. This feature has apparent benefits for individuals who struggle with alcoholism or abstain from drinking due to religious beliefs. As Ad Age noted, “this is the first time anyone can proactively block a topic” (Sloane 2016). Before, users could only manage topics after they were served an ad. The article mentions Facebook’s plans to also hide ads "For families who experience the loss of a child, to continue to see ads about parenting and new baby stuff, that can be really upsetting" (Sloane 2016). This tool is one step in the right direction for monitoring ad targeting, since control is given back to the user and prevents negative consequences of ad targeting.

While every Facebook user has the opportunity to manage his or her Ad Preferences, most users are unaware of this capability. Large publications such as Business Insider, The Washington Post, and The New York Times have written articles about Facebook Ad Preferences, yet most users are unaware of its existence.

Snapchat

Snapchat is a young social media platform that has grown exponentially in the past year. Evan Spiegel created the platform in September 2011. In his first blog post, Spiegel said, "Snapchat isn't about capturing the traditional Kodak moment. It's about communicating with the full range of human emotion—not just what appears to be pretty or perfect” (Spiegel 2011). Unlike Facebook and Twitter, photos and messages shared on Snapchat encourage users to

communicate in the now. Once a user opens a picture, they have a maximum of 10 seconds to view, or it 'erases' forever. This non-committal format has attracted millennials to the platform. According to a 2015 study, "Snapchat reaches 41% of all 18 to 34 year olds in the United States." (Nielsen 2015). Since that study, Snapchat has only grown. With increased concerns over online privacy, Snapchat presents itself as a more secure option. Snapchat claims:

> "From the beginning, the way we treat your information has been very different from other technology companies. We don't stockpile your private communication, and we don't show your friends an ongoing history of everything you've ever posted. We believe that this approach makes the Snapchat app feel less like a permanent record, and more like a conversation with friends."

Through this, Snapchat has shaped its own path in the social tech industry. They are one of the few apps that have stayed independent from large companies like Google and Facebook. Snapchat even turned down a $3 billion offer from Facebook in 2014. That decision has proved beneficial, considering speculators value Snapchat up to $28 billion now. This value is more than nine times Facebook's offer (Helmore 2017). The growth is the company is mainly due to the introduction of Snapchat's Discover in January 2015 following its first form of advertising in October 2014. Discover features a collection of branded stories by major publications ranging from Buzzfeed and Cosmopolitan to The Economist and The Wall Street Journal. Widespread monetization of Snapchat was first introduced through ad placements in these branded stories.

Snapchat's relationship with advertising has evolved tremendously through the years. At first, Snapchat was adamant about "not being creepy" (Spiegel 2015). At Cannes Film Fest in 2015, Snapchat CEO reiterated that Snapchat had no plans to go too far in targeting (Shields 2015). The app sold advertisements through contextual targeting, socio-demographic targeting (age and gender), geographic targeting, and technical targeting (device use). With contextual targeting,

advertisers could select different publishers depending on their brand. "[Advertisers] can opt for audience 'bundles,' which are packages of Discovery channels grouped by a theme such as 'world news and culture,' which compiles CNN, Mashable, Vice, and National Geographic" (O'reilly 2015). However, with competitors such as Facebook using hyper-targeted advertising, advertisers were reluctant to advertise with Snapchat. In fear of invading its users privacy, Snapchat was reluctant to use common behavioral targeting techniques. As of January 2017, Snapchat's Private Policy states:

> "We want you to feel understood. We want to understand what's relevant to you and your life, and we want to show you things that you'll care about. At the same time, we don't want to serve ads that are so custom-tailored that they feel invasive or uncomfortable. It's a difficult balance and we may not always get it right, so we are counting on Snapchatters for feedback; please consider sharing your experiences with us."

As Snapchat prepared to become public, it changed its advertising policy to allow advertisers to use third party data for targeting. Through a partnership with Oracle Data Cloud, brands can apply data from offline purchases, such as supermarket loyalty cards, to better target consumers. Advertisers will also be able to use Oracle's data to "measure whether Snapchat ad campaigns result in real-world sales" (Shields 2017). The big question is whether Snapchat users understand the implications of this partnership.

In early March 2017, Snap Inc., Snapchat's parent company, finally went public. Since then, Snapchat has taken steps to increase the number of brands who advertise on the platform. Business Insider reports, "Starting this June, Snap is going a step further by flinging wide its gates to advertisers of all sizes and budgets with a new suite of self-service tools. The move could help considerably grow Snap's fledgling ad business, which is expected to reach $1 billion in revenue this year" (Heath 2017). Self-service tools will broaden and diversify brands that

advertise on the platform. Since there is not a minimum ad spend, advertisers with smaller budgets will now be able to reach Snapchat's competitive demographics. The new ads manager has options for app install ads, sponsored geo-filters, and full screen video. In beta form, the ad manager allows brands to "use your customer data like emails or mobile advertising IDs to effectively reach Snapchatters" (Heath 2017). Snapchat appears to have a similar set-up to Facebook in which advertisers can either target "Snap Audience Match" to reach specific individuals or "Lookalike Audience" to expand their reach. Both features are a clear departure from Evan Spiegel's earlier thoughts on advertising.

Transparency

Similar to Facebook's "Ad Preferences," Snapchat users can have a peek into the personal information collected by Snapchat. Accessing this information is not as seamless as Facebook, but it is relatively simple. Users "go to accounts.snapchat.com, click My Data, and [Snapchat] will let [the user] know when [their] information is ready to be downloaded" (Snapchat 2017). The information is then sent to the user's email as an attachment. Once downloaded, there are 6 html links to "account," "purchase history," "shared story," "support note," "snap history" and "user profile." Through snap history, users can view a long list of the snaps sent and received. While the actual image or message is not available to view, users can see the exact time an image was sent or received and to which user. This proves that Snapchat maintains a trace of every snap sent, a fact some Snapchatters might not fully understand. In "User Profile," users can see the total time spent and total view count of different brand's advertisements. It provides the user's frequent locations as well as an individual's latest location. Lastly, there is a list of interest categories. Some examples of potential categories are "Hipsters & Trendsetters," "News Watchers," and "Collegiates." Compared to Facebook, these categories are much broader and

less intrusive. Although Snapchat is built to feel safe and untraceable, users' conversations are not as private as users might think. The platform keeps data on its users by tracking whom a user talks to, how often, and where. As the company shifts from private to public this year, it is important to track how their privacy will shift.

In the last five years, there has been growing concern regarding government entities invading individual's online privacy. Snapchat confronts these concerns by being transparent about their cooperation with U.S. officials. "Snapchat Transparency Reports are released twice a year. These reports provide important insight into the volume and nature of governmental requests for Snapchatters' account information and other legal notifications." Between January 1, 2016 and June 30, 2016, Snapchat received 1472 (761 request during same period in 2015) requests from government agencies. These request affected 2455 total users (1286 accounts in 2015). Out of the 2016 requests, Snapchat produced data for 82% of the requests. Snapchat's cooperation with officials demonstrates how private data does not always stay private. For advertising, this demonstrates that Snapchat has a lot more insight into user behaviors than it might openly discuss with users.

Advertising Rules

When it comes to age, Snapchat follows typical advertising practices toward children. "Our services are not intended for—and we don't direct them to—anyone under 13. And that's why we do not knowingly collect personal information from anyone under 13." Snapchat is a relatively new app, "60% of users are under 25, and nearly a quarter (23 percent) have not yet

graduated from high school" (Statista 2016). Since their demographic skew young, Snapchat should be extra cautious when it comes to advertising.

Similar to Facebook, Snapchat has restrictions on what brands can advertise. Snapchat policy is that "all ads are subject to our review and approval. We reserve the right to reject or remove any ad in our sole discretion for any reason. We also reserve the right to request modifications to any ad, and to require factual substantiation for any claim made in an ad." three main type of restrictions exist: prohibited content, prohibited ads, and restricted ads.

Snapchat's Ad Restrictions

Prohibited Content	Content that promotes Snapping and driving, or otherwise encourages dangerous behavior;
	Content that demeans, degrades, or shows hate toward a particular race, gender, culture, country, belief, or toward any member of a protected class;
	Content that exploits an individual who is drunk or otherwise intoxicated;
	Content depicting nudity, sexual behavior, or obscene gestures;
	Content depicting drug use;
	Content depicting excessive violence, including the harming of animals;
	Shocking, sensational, or disrespectful content;
	Deceptive, false, or misleading content, including deceptive claims, offers, or business practices;
	Content that directs users to phishing links, malware, or similarly harmful codes or sites; and
	Content that deceives users into providing personal information without their knowledge, under false pretenses, or to companies that resell, trade, or otherwise misuse that personal information.
	Companies that resell, trade, or otherwise misuse that personal information.
Prohibited Ads	Adult products and services (other than contraceptives; see below);
	Cigarettes (including e-cigarettes), cigars, smokeless tobacco, and other tobacco products;
	Products or services that bypass copyright protection, such as software or cable signal descramblers;
	Products or services principally dedicated to selling counterfeit goods or engaging in copyright piracy;
	Get-rich-quick or pyramid schemes or offers or any other deceptive or fraudulent offers;
	Illegal or recreational drugs or drug paraphernalia;
	Counterfeit, fake or bootleg products, or replicas or imitations of designer products;
	Firearms, weapons, ammunition, or accessories;
	Ads that promote particular securities or that provide or allege to provide insider tips;
	Ads targeted to countries subject to U.S. trade sanctions and other U.S. export control laws; and
	Any illegal conduct, product, or enterprise.
Restricted Ads	Ads that promote or reference alcohol;
	Ads for online dating services;
	Ads for gambling and games of skill;
	Ads for lotteries;
	Ads for financial services;
	Ads for contraceptives;
	Ads for online pharmacies or pharmaceuticals;
	Political ads, which are currently allowed only in the United States and are subject to Snapchat's Political Advertising Guidelines; and
	Ads promoting dietary and herbal supplements.

LinkedIn

LinkedIn is a social network and online platform for professionals. The company was founded in December 2002, two years prior to Facebook. Today, Microsoft owns the company after a successful acquisition on December 8, 2016. The platform is used across the world for job networking and recruiting purposes. As of Fall 2016, there are 433 million registered LinkedIn users (Blake 2016). The company refers to LinkedIn users as Members. Out of the 433 million registered Members, 70% are located outside of the United States. In comparison with other social media platforms, the majority of users spend less time accessing this site; only 40% of LinkedIn users check the site daily (Blake 2016). Unlike Facebook and Snapchat, LinkedIn is a social media platform skewed more towards the educated upper class. Based on a 2017 Pew Research study, 77% of LinkedIn users have an annual household income greater than $50,000 and half of users have some college degree (Pew Research Center 2016). Additionally, 67% of LinkedIn users describe themselves as "news junkies" (Blake 2016). Although the site predominately attracts one subset of society, its age breakdown is fairly even. The age distribution for LinkedIn users is 18-29 (34%), 30-49 (33%) 50-64 (24%), 65+ (20%) (Pew Research Center 2016).

Private Policy Overview

Like other social media platforms, LinkedIn has monetized off users data. The site has a thorough online private policy that lies the foundation of what information can be collected and how that information can be shared. The core tenant of LinkedIn's privacy policy is user trust because according to the platform, "trust is what powers the LinkedIn professional network" (LinkedIn 2017). All privacy decisions are based around and explained through this concept. The first thing shown on LinkedIn's privacy policy is a video outlining the purpose of its policy. In it, users are

reminded that a privacy policy should be "easy to understand, and centered around protecting [...] members to ensure [LinkedIn] continues to earn [users'] trust" (LinkedIn 2017). The video claims LinkedIn achieves this by giving users "clarity, consistency, and control over [their] information" (LinkedIn 2017). Even before getting into specific details, LinkedIn clearly states, "we never rent sell or distribute your private information to third parties unless you ask us to" (LinkedIn 2017). The site updates their Privacy Policy regularly. When changes are made, users may or may not be notified. The site claims it is the user's responsibility to read through the Privacy Policy and "continuing to use [LinkedIn] Services after [LinkedIn] publish or communicate a notice about any changes to this Privacy Policy means that [users] are consenting to the changes" (LinkedIn 2017).

If users disagree with LinkedIn's Privacy Policy, they are asked to close their account (LinkedIn 2017). As LinkedIn is a major source for jobs and networking, this put users in a difficult situation. In 2013, roughly ninety-four percent of recruiters used LinkedIn to vet potential candidates (AdWeek 2013). By leaving LinkedIn due to privacy concerns, job seekers miss out on job positions. There are, however, some capabilities to opt out and limit data collection. These will be discussed in a later section.

Third-Party Data Sharing

LinkedIn states they will protect user's personal information and only provide data to third parties "(1) with user's consent; (2) by a user's request; (3) to carry out LinkedIn necessary functions; (4) when required by law; (5) "as necessary to enforce our User Agreement or protect the rights, property, or safety of LinkedIn, our Members and Visitors, and the public" (LinkedIn 2017).

The site also claims they "do not share your personal information with any third-party advertisers or ad networks for advertising without [a user's] separate permission" (LinkedIn 2017). However, personal information is not explicitly defined in the site's Privacy Policy.

What Data is Collected

There are ten main categories of data that LinkedIn collects. They range in security and complexity.

Registration	When a user registers for LinkedIn he must provide a name, email, mobile number, and password
Profile information	Users build a profile that includes skills, professional experience, educational background, honors, awards, professional affiliations, group memberships, networking objectives, companies or individuals he follows, other information including content
Address Book and other Service that Sync with LinkedIn:	If a user syncs a contact list with LinkedIn, the platform stores their contacts emails and phone numbers. If LinkedIn is used on a mobile device, users can sync with their device's calendar, email, and contact apps.
Customer Service:	LinkedIn stores data on customer service conversation to enhance their platform. However, none of this information is allowed to be sold for advertising.
Using the LinkedIn sites and applications:	LinkedIn owns other sites and applications such as SlideShare and Pulse. LinkedIn collects data from those sites and creates rich user profiles by combining site history based on IP addresses and cookies. "Even if [a user is] not logged into a Service, we log information about devices used to access our Services, including IP address"
Using third-party services and visiting third-party site	The site uses tracking information collected by third-party services and visiting third-party sites. This is applied to all users unless he manually opts out.
Cookies	The platform states, "by visiting our Services, [a user] consent[s] to the placement of cookies and beacons in [his] browser and HTML-based emails in accordance with this Privacy Policy" (LinkedIn 2017). LinkedIn uses two forms of cookies: persistent cookies and session cookies. Persistent cookies track users over a period of time, whereas session cookies track users only for the length of a session. Cookies are the main tool used to recognize users across different services and gain insight into user behavior once off LinkedIn.com. Cookies are beneficial for advertisers because they track the effectiveness of ad campaigns.

Advertising technologies and web beacons	LinkedIn provides a thorough explanation on how data associated with advertising is collected and used. Like Facebook and Snapchat, LinkedIn allows brands to serve targeted ads. To create targeted ads, LinkedIn makes inferences on their users based on information from their profile, how a user uses their services, and from information provided by third parties. From a Member's profile, information is inferred about the individuals "for example, using job titles to infer age, industry, seniority, and compensation bracket; or names to infer gender" (LinkedIn 2017). Information stored from how a member uses their site includes search history, content a user reads, page visits, how a user interacts with an ad, etc. Information from third parties comes from advertising partners, publishers, and data aggregators. LinkedIn combines third party data with data collected from their site to create a detailed interpretation of each user.
Devices and Networks you use	LinkedIn collects data on the type of operating system and device used when accessing their site. This also includes IP addressses.
Other	

Prohibited Advertising

LinkedIn has a series of guidelines set in place to reduce unethical advertising practices. Additionally, many of these guidelines contain the clause "even if legal in the applicable jurisdiction" (LinkedIn 2016). This demonstrates LinkedIn's continuous dedication to creating a trustworthy platform, beyond the necessary limits set forth by the government.

One example of LinkedIn's prohibited types of advertising is ads that foster discrimination in hiring and education. The site does not "allow ads that advocate, promote or contain discriminatory hiring practices or denial of education or economic opportunity based on age, gender, religion, ethnicity, race or sexual preference" (LinkedIn 2016). The site also does not allow any form of advertising that includes "hate speech or show or promote violence or discrimination against others or damage to their property or are personal attacks on any individual, group, company or organization or otherwise advocating against or targeting any individual, group, company or organization" (LinkedIn 2016). LinkedIn prohibits offensive and inappropriate language in all of their ads and deciding whether certain language is appropriate depends on LinkedIn employees. LinkedIn also prohibits ads that are

"offensive to good taste" (LinkedIn 2016). Through this clause, LinkedIn has greater and more flexible control on ads that might not directly go against earlier stated guidelines. The site is also allowed to reevaluate whether an ad is appropriate depending on current events and societal climate. Through these guidelines, LinkedIn goes beyond the law and implements rules that protect its users.

For political advertising, all ads must "clearly identify the person or entity that paid for the message" (LinkedIn 2016). Furthermore, "ads not financed by a candidate or campaign must indicate whether the content is authorized by a candidate and, if not, include contact information for the person or entity that paid for the message" (LinkedIn 2016). This brings transparency to LinkedIn's members and ensures political ads are accurately representative of the candidate.

The last guideline is perhaps LinkedIn's most significant one. It states LinkedIn prohibits ad targeting based on "sensitive categories such as inferred or actual information regarding financial status, alleged/actual commission of a crime, health, political affiliation/beliefs, racial or ethnic origin, religious or philosophical affiliation/beliefs, sexual behavior or orientation, or trade union membership" (LinkedIn 2016). Including inferred information to this guideline is important because, in theory, it prevents advertisers from making inferences on income or beliefs based on a user's job position or online behaviors. However, this guideline is in stark contrast to another statement in LinkedIn's Privacy Policy. In 1.9, LinkedIn admits to collecting user data for advertisers to purchase. The platform admits to collecting "information inferred from a Member's profile (for example, using job titles to infer age, industry, seniority, and compensation bracket; or names to infer gender)" (LinkedIn 2017). Essentially, this clause would allow advertisers to make assumptions on a Member's income before a Member discloses that information.

Restricted Advertising

Similar to Facebook and Snapchat, LinkedIn has a series of restrictions on advertisements.

Restricted Advertising	Illegal Products and Services; Fake Documents and Related Services; Offensive Products and Services; Alcoholic Beverages; Tobacco Products or Cigarettes; Drugs, Illegal Substances and Related Products; Weapons, Firearms, Ammunition, Fireworks or any Oth Violent Products or Services; Sexual or Adult Content; Sexual or Adult Products or Services; Dating Services; Ringtones and Video Games; Illegal Downloads of Software, Media or Other Copyrighted Content; Gambling, Sweepstakes and Virtual Currency; Scar Occult Pursuits; Endangered Species and Fur; Health Matters; Harmful to LinkedIn or its Members; Affiliate Advertising; Soliciting Funds; Financial Products

Opting Out

LinkedIn members and non-members have easy access to opt out of data collection and personalized targeting. LinkedIn, "gives [users] a number of ways to opt out of targeted ads, including through the Ad Choices icon shown with any ads we serve on third-party sites" (LinkedIn 2017). Individuals who do not actively opt-out give "consent to [LinkedIn's] use of beacons and other advertising technologies" (LinkedIn). While opt-out functions are available through LinkedIn, the platform heavily discourages users from utilizing this function. The social platform makes clear that individuals who opt-out will still receive advertisements, but those advertisements will not be targeted based on their online behaviors and inferred interests. Addressing disclaimers above, members that disagree with LinkedIn's advertising policies are asked to close their account, but LinkedIn argues, "there is no need to do that because we've worked hard earn the trust of millions of professionals" (LinkedIn 2017). LinkedIn uses persuasive messaging to convince its users to keep its targeting features. While the platform relies on the trust of its Members, revenue comes from selling its data. Therefore, LinkedIn wants to keep collecting data on the majority of its Members to stay profitable. Although LinkedIn cares about its Members, the needs of the company take priority.

In LinkedIn's opt-out section, the platform addresses Federal Trade Commission's, FTC, promoted "Do Not Track" policy. This policy "implements a mechanism for allowing Internet users to control the tracking of their online activities across websites by using browser settings" (LinkedIn 2017). While attempts have been made to enforce this policy, there are no current standards in place. Since there is no industry standard, "LinkedIn does not generally respond to "do not track" signals" (LinkedIn). LinkedIn's decision to overlook "do not track" signals demonstrates the lack of enforcement by the Federal Trade Commission.

Chapter 4: Big Data

The root of all behavioral targeting is data. Broken down, the more data a brand has on a certain individual, the more precise an advertiser can be. Today, this data is collected and combined across devices and mediums. Social platforms play a singular role in a greater media landscape. Each time an individual goes online, purchases an item with a credit card or loyalty card, data is collected on him.

Data Brokers

Understanding Big Data means understanding the companies that buy, sell, and control the data. These companies are called data brokers and collect personal information on almost every American individual. "For example, one [...] data broker has 3000 data segments for nearly every U.S. consumer" (FTC 2014). However, "because these companies generally never interact with consumers, consumers are often unaware of their existence, much less the variety of practices in which they engage" (FTC 2014). This is by no means a mistake. By staying relatively unknown to the general population, data brokers make a large profit on selling data to advertisers and brands. They "collect personal information about consumers from a wide range of sources and provide it for a variety of purposes, including verifying an individual's identity, marketing products, and detecting fraud" (FTC 2014). However, data brokers do not collect this information directly from consumers. Instead, they purchase or access consumer information through "government sources; other publicly available sources; and commercial sources" (FTC 2014). To bring greater transparency to data brokers and their role in online privacy, the Federal Trade Commission conducted an in-depth study into nine different data brokers.

Nine Data Brokers

Acxiom	Acxiom provides consumer data and analytics for marketing campaigns and fraud detection. Its databases contain information about 700 million consumers worldwide with over 3000 data segments for nearly every U.S. consumer.
Corelogic	Corelogic provides data and analytic services primarily on property information, as well as consumer and financial information. Its databases include over 795 million historical property transactions, over ninety-three million mortgage applications, and property-specific data covering over ninety-nine percent of U.S. residential properties, in total exceeding 147 million records.
Datalogix	Datalogix provides businesses with marketing data on almost every U.S. household and more than one trillion dollars in consumer transactions. In September 2012, Facebook announced a partnership with Datalogix to measure how often Facebook's one billion users see a product advertised on the social site and then complete the purchase in a brick and mortar retail store.
eBureau	eBureau provides predictive scoring and analytics services for marketers, financial services companies, online retailers, and others. eBureau primarily offers products that predict whether someone is likely to become a profitable customer or whether a transaction is likely to conclude in fraud. It provides clients with information drawn from billions of consumer records, adding over three billion new records each month.
ID Analytics	ID Analytics provides analytics services designed principally to verify people's identities or to determine whether a transaction is likely fraudulent
Intelius	Intelius provides businesses and consumers with background check and public record information. Its databases contain more than twenty billion records.
PeekYou	PeekYou has patented technology that analyzes content from over sixty social media sites, news sources, homepages, and blog platforms to provide clients with detailed consumer profiles.
Rapleaf	Rapleaf is a data aggregator that has at least one data point associated with over eighty percent of all U.S. consumer email addresses. Rapleaf supplements email lists with the email address owner's age, gender, marital status, and thirty other data points.
Recorded Future	Recorded Future captures historical data on consumers and companies across the Internet and uses that information to predict the future behavior of those consumers and companies. As of May 2014, Recorded Future had access to information from over 502,591 different open Internet sites. (FTC 2014)

Reading through each company's description, it appears as if the companies operate in isolation from one another. This is far from reality. The risk associated with data brokers is not from one company's data set; it's from the combination of different data that unlock personal information

on users. Social media data collected from PeekYou can be combined with background check data from Intelius to make assumptions about how different interest groups on Facebook can predict a person's criminal record. Simply put, the sum is greater than its parts. "While each data broker source may provide only a few data elements about a consumer's activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer's life" (FTC 2014). Through the study, the Federal Trade Commission found that "seven of the nine data brokers buy from or sell information to each other" (FTC 2014). By combining multiple data sets, each data broker has a comprehensive understanding of singular individuals.

Through detailed analysis on consumers, data brokers segment individuals into highly specialized consumer groups. For example, if data brokers view a group with similar patterns of buying health bars, riding their bike to work, and buying socially responsible clothes, they would hypothetically bundle this group together as "Consciously Actives." Advertisers selling KIND Bars could then contact a data broker and buy data associated with this consumer interest group. Data can range from email addresses, home addresses, and IP addresses. Brands will then combine these consumer segments to first-party information collected offline, connecting the digital world with the physical world. This process is called "onboarding" and "refers to a process whereby a data broker adds online data into a cookie (the process of onboarding online data) to enable advertisers to target consumers virtually anywhere on the Internet" (FTC 2014). With onboarding, advertisers have a holistic understanding of their consumer that can be used to create highly targeted and specialized ads.

This process is a fairly common practice within the advertising world and enables interest-based targeting. The argument for interest-based targeting is increased relevancy to the consumer. In

return, advertisers can serve highly specialized targeting. Some real consumer interests groups found from the FTC's 2014 study were fairly harmless like "Dog Owner, Winter Activity Enthusiast, or Mail Order Responder" (FTC 2014). These practices allow advertisers to effectively spend their budget by only spending advertising dollars on individuals who typically purchase their products. As discussed later in chapter six, most individuals would not have a problem with this level of segmenting because it categorizes based on low-risk, relevant interests.

The concern with this practice is when interest groups enter sensitive categories. The 2014 FTC study uncovered real interest groups that "focus on ethnicity and income levels, such as "Urban Scramble" and "Mobile Mixers," both of which include a high concentration of Latinos and African Americans with low incomes" (FTC 2014). In another instance, data brokers created an interest group for upper middle class individuals with no children called "Married Sophisticates" (FTC 2014). While these segments allow advertisers to target people who are more likely to buy their products, it is a low-level form of discrimination. By limiting exposure of luxury items to lower income individuals, aspirations are also limited. On the flip side, wealthy individuals should have the opportunity to see ads for discounts and sales. Other sensitive categories such as "Diabetes Interest and Cholesterol Focus" enter a series of ethical concerns and questions on whether advertisers should be able to advertise based on health-related topics (FTC 2014).

Not only is interest based targeting discriminatory in nature; it can cause harm if inaccurately inferred. One example by the FTC was "a data broker could infer that a consumer belongs in a data segment for "Biker Enthusiasts," which would allow a motorcycle dealership to offer the consumer coupons, an insurance company using that same segment might infer that the

consumer engages in risky behavior" (FTC 2014). Using the category Diabetes Interest, "a manufacturer of sugar-free products could use to offer product discounts, an insurance company could use that same category to classify a consumer as higher risk" (FTC 2014). These examples expose risks associated with making inferences off of seemingly harmless data sets.

Advocates against businesses using Big Data argue that Big Data strips many freedoms away from the consumer. Even consumers who are aware of Big Data practices can do little to prevent companies from collecting, selling, and using their information for marketing. This is because of the complex nature of sharing data. Since data is sold through several data brokers before eventually being used by advertisers, it is near impossible to pinpoint the source of a consumer's information. By the time an advertiser obtains information on an individual, that information could have passed through several companies' data banks. The FTC claims "it would be virtually impossible for a consumer to determine how a data broker obtained his or her data; the consumer would have to retrace the path of data through a series of data brokers" (FTC 2014). While social media platforms preach a privacy policy rooted in transparency, the data broker they partner with heavily benefit off obscurity.

Following the study, the FTC had three main recommendations for the federal government. First, the Commission recommended legislation that "enable consumers to easily identify which data brokers may have data about them and where they should go to access such information and exercise opt-out rights" (FTC 2014). Second, Congress should require data brokers to "clearly disclose to consumers (i.e., on their websites) that they not only use the raw data that they obtain from their sources, [...] but that they also derive from the data certain data elements" (FTC 2014). Enforcing these recommendations would shine light on how sensitive data such as a

person's name or age could be coupled with other data sets to create more comprehensive data inferences. Third, legislation should be implemented that required "data brokers to disclose the names and/or categories of their sources of data" (FTC 2014). By identifying the source, consumers would have greater transparency into where their information was being collected and shared. This would also allow consumers to correct any incorrect information at the source. Finally, Congress should make data brokers disclose the limitations of opt-out and require "consumers' affirmative express consent before they collect sensitive information" (FTC 2014). Since most individuals are unaware of the implications of Big Data, a notice from data brokers will increase the opportunity for consumers to make an educated decision. Through these measures, the Federal Trade Commission hoped to return control back to the consumer and take a step towards greater transparency.

As noted in the report, protecting individuals' private data is especially crucial in this day and age. Every additional technology platform introduces a new way to track and collect an individual's data. For perspective, tools can now track behaviors across devices so that "companies can communicate a timely message tailored to a consumer based on the consumer's location" (FTC 2014). More recently, the introduction of artificial intelligence, AI, into the household through products like Amazon Echo and Google Home has allowed for constant audio surveillance of individuals. All of these products create more opportunities for brands and advertisers to understand their consumer. The question remains, at what cost to the consumer?

Personally Identifiable Information (PII)

In January 2014, Pew Research Center did a survey regarding the state of privacy and privacy awareness in the United States .The study included 607 American adults, age 18 and older. According to the study, "80% of those who use social networking sites say they are concerned about third parties like advertisers or businesses accessing the data they share on these sites" (Pew Research Center 2014). One way to prevent businesses from accessing personalized data is by using anonymization. However, "Just 24% of adults "agree" or "strongly agree" with the statement: "It is easy for me to be anonymous when I am online" (PewResearch 2014). The majority of individuals have the right idea about a lack of anonymity online. One journal article, *Goodbye PII: Contextual Regulations for Online Behavioral Targeting*, carefully lays out how true anonymity doesn't exist because of the existence of Big Data.

One privacy researcher, Yuen Yi Chung, attributes flawed U.S. privacy laws to the concept of PII, or Personally Identifiable Information. PII is what has served as the basis of all preventative privacy laws since 1970. Defining what is classified as PII is no a simple feat. There is large confusion and debate over what is and what is not personally identifiable information. Today, there are three main ways to define PII. First is the Tautological Approach. This approach suggests PII triggers protection is "any information that identifies a person" (Chung 2014). The vagueness of this definition creates more confusion than clarity. The second approach is a non-public approach that defines PII by defining what it is not, public information. Chung argues, "this approach is problematic because it fails to take into account whether such information is identifiable and overlooks the possibility that other nonpublic information may readily be matched to this type of public information" (Chung 2014). The third option is the Specific-Types

approach that claims PII is anything that allows someone to access a certain individual. This approach does not account for data sharing by brokers. Without one clear definition for PII, advertisers and brands can interpret privacy laws to best suit their goals and needs.

As previously mentioned, one main tool to escape PII laws is for brands and companies to adopt anonymous practices. "Even if information falls within the scope of PII, Congress permits a more flexible regulatory system as long as such data is anonymous. Therefore, sensitive information may be traded publicly as long as the data administrator makes the PII unidentifiable" (Cung 422). The reality is that data cannot be fully anonymous. Chung provides three case studies that demonstrate how sensitive information can be pulled from specific individuals simply from public information or combining other data sets. The process of taking anonymous data and combining it with other data sets, either private or public, is known as re-identification. Re-identification is a process that inhibits privacy and can lead to sensitive information being unrightfully released. Three cases below prove the key limitation of anonymization:

Simple Demographics Can Uniquely Identify Us:

In 1990, Latanya Sweeney, a professor of computer science at Carnegie Mellon University compared the 1990 census with a few unique characteristics accessed through third party data. Sweeney found that 87.1% of U.S. individuals could be identified through just three pieces of public information: zip code, gender, and birth date. The study was repeated in 2000, with researchers finding that only 63% of U.S. individuals could be identified (Chung 2014). Even with this decline in accuracy, more than half of the population could still be identified through

easily accessible data. To prove the potential harm of this ability, Sweeney identified her governor's medical record history.

In terms of social media, Facebook's Ad Preferences indicates a user's birthday, gender, and current location (zip code), which can all technically be sold to advertisers. Using Sweeney's research methods, there is little doubt that brands could correctly identify the majority of individuals targeted.

The Netflix Prize Surprise:

In 2006, Netflix hosted a contest for developers to create an algorithm that would improve the accuracy of movie recommendations. "The company released 100 million rental records from nearly half a million users - and offered a bounty of a million dollars to anyone that could improve its film recommendation by at least 10 percent" (Mayer-Schönberger) While Netflix's intended goal was to improve movie recommendations, there was a bigger, unforeseeable result. Researches at the University of Texas at Austin compared the privately released Netflix data against public information. "By cross referencing a user's public IMDB ratings and user information, along with the private database released by Netflix, one may deduce a user's real identity, along with sensitive information such as political views, religion and sexual orientation" (Chung 2014). Specifically, the researchers found that "rating just six obscure movies could identify a Netflix customer 84 percent of the time" (Mayer-Schönberger). Additionally, if data on which a person rated the movie was known, researchers could identify an individual "among the nearly half a million customers in the dataset with 99 percent accuracy"(Mayer-Schönberger). For proof, the researchers accurately re-identified "Jane Doe," a closeted lesbian and mother living in America's conservative Midwest. It only took two separate, but connected,

data sets to accurately identify Jane Doe. “In theory, anonymization is the ideal protection for data if there were no external sources to cross-reference. In reality, a wide range of information about people is available through many easily accessible means” (Chung 429). This case study demonstrates how seemingly harmless data can be used to infer sensitive information.

AOL Research Shows You Are What You Search:

Like Netflix, American Online (AOL) released a vast amount of private data in 2006. In an initiative called “AOL Research,” the company released “twenty million search queries for over 650,000 individuals that used its search engine over a period of three months” (Chung 2014). While the data released included private searches, the company removed usernames and IP addresses in the attempt to protect the data. When the data was first released, there were some critiques that AOL had broken privacy laws. AOL responded by saying there was no violation of privacy because there was “no linkage between the anonymized queries and actual individuals” (Chung 2014). Researchers could look at the data and see patterns between users and their search history, but AOL claimed an actual identity could not be identified. This claim was shattered within days when *The New York Times* successfully identified user number 4417749 as Thelma Arnold. Arnold was a 62-year-old from Georgia who had recently searched for “60 single men” and “tea for good health” and “landscapers in Liburn, Ga” (Mayer-Schönberger). She was easily identified because of the content of her searches. Arnold was shocked when the *New York Times* contacted her, claiming “My goodness, it’s my whole personal life [...] I had no idea somebody was looking over my shoulder” (Mayer-Schönberger).

Perfect Anonymization is Impossible

All three companies hindered their users' privacy because they did not recognize the limitations of anonymization. Through Big Data, individual information can be de-anonymized and re-identified. As the amount of data increases, the easier it will become to identify unique individuals. Paul Ohm, a professor at Georgetown University, is an expert on harm done by de-anonymization. He claims, "given enough data, perfect anonymization is impossible no matter how hard one tries" (Mayer-Schönberger). Ohm coined the term "Database of Ruin," for the "worldwide collection of all information held by third parties, that may be used to probe into private lives" (Chung 2014). Within this single, powerful database, Ohm claims that it only takes one connection between a piece of data and someone's personal identity to decode any other anonymized databases. This is why linking even non-sensitive information can lead to the linking of highly private and sensitive information. Ohm declares this is why "re-identification techniques defeat the purpose of almost every privacy law and regulation in the U.S." (Chung 2014).

Chapter 5: Privacy Law and Self-Regulations

Current U.S. laws regarding privacy all revolve entirely around anonymization. Chung argues "Congress has just used anonymization in order to avoid making a real decision in balancing privacy interests." (Chung 433). Companies are encouraged to use one of three main strategies to ensure privacy: individual notice and consent, opting out, and anonymization. However, none of these practices fully address the problem. If linking data is inevitable, perhaps the focus on privacy should not be *if* people can access secure information but rather, the focus should be *how* people can use data.

Currently, there are no explicit privacy laws in the U.S. regarding data-driven targeting. There have been several attempts to enact legislation regarding advertisers use of private information. In February 2011, "Do Not Track Me Online Bill" was proposed as an online version of "Do Not Call" law. It would allow users an opt-out option for online tracking of personal information. This personal information included names (i.e. address, e-mail address, etc.) government issued identification (i.e. Passport, drivers license, etc.), and financial account numbers (credit card, debit cards, etc.). The bill also forbid data collection over medical history, race or ethnicity, religious beliefs, sexual orientation, income, precise geo-location, biometric data, and social security number. This bill was ultimately not enacted.

Following failure of the bill, the Obama administration introduced the Consumer Privacy Bill of Rights in 2012 and 2015. President Obama introduced the need for a Bill of Rights by saying:

> "As the Internet evolves, consumer trust is essential for the continued growth of the digital economy. That's why an online privacy Bill of Rights is so important. For businesses to succeed online, consumers must feel secure. By following this blueprint,

> companies, consumer advocates and policymakers can help protect consumers and ensure the Internet remains a platform for innovation and economic growth."

The Consumer Privacy Bill of Rights ensured individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability (The White House 2012). The administration claimed that enacting the Consumer Privacy Bill of Rights would "increase legal certainty for companies, strengthen consumer trust, and bolster the United States' ability to lead consumer data privacy engagements with our international partners" (The White House 2012). The White House further noted, "even if Congress does not pass legislation, the Consumer Privacy Bill of Rights will serve as a template for privacy protections that increase consumer trust on the Internet and promote innovation" (The White House 2012). The proposal was widely criticized, and never implemented.

Near the end of President Obama's term, federal officials implemented new rules to protect consumers' online privacy. Through the Federal Communications Commission rule, broadband providers were limited on what type of consumer data they could share. The rule was voted on by the FCC's five commissioners and passed 3-2 (Fung 2016). Various types of sensitive consumer data such as browsing history, app usage, location data, and other information could not be shared or sold to outside individuals. Additionally, the FCC vote restricted, "trading in health data, financial information, Social Security numbers and the content of emails and other digital messages. [Under this rule, service providers must disclose] what data they collect and why, as well as to take steps to notify customers of data breaches" (Fung 2016). While this took steps towards limiting the abuse of consumer privacy, Republican opponents said this was an unfair disadvantage to broadband companies and created an advantage to "Google and Facebook that already make billions of dollars collecting data on users and selling it to advertisers" (Fung

2016). Advocates of the ruling said the FCC was taking steps in the right direction by beginning to regulate online data-driven targeting with industries that have the most sensitive amount of information, and therefore the greatest amount of harm.

Due to these critics, the Trump Administration has taken drastic measures to rollback rulings implemented by the Obama Administration. On March 28, 2017, the United States House of Representative had a party-line vote, 215-205, against the Federal Communications Commission Rule. The ruling eliminated the government's authority to protect consumers' private information from being sold or used by broadband companies like AT&T, Verizon, Comcast, etc. Republican representatives, eager to remove regulations implemented by President Obama, fully supported the vote. On the opposing side, Nancy Pelosi, Minority Leader for the Democratic Party, staunchly opposed the vote and told reporters, "Overwhelmingly, the American people do not agree with Republicans that this information should be sold, and it certainly should not be sold without your permission" (Freking 2017). Following the vote, Jeffrey Chester, Executive Director of the Center for Digital Democracy said, "Today's vote means that Americans will never be safe online from having their most personal details stealthily scrutinized and sold to the highest bidder" (Fung 2017). While Democrats claim Republicans exploited individuals' privacy rights for profits, Republicans insist they are protecting competitive fairness and the privacy of individuals.

Ajit Pai, the Trump-appointed Chairman of the FCC, is a "critic of the broadband privacy rules and has said he wants to roll them back" (Freking 2017). Instead of implementing broadband privacy rules, Pai wants the Federal Trade Commission, not the Federal Communications Commision, to police privacy for broadband companies and internet companies. Another

republican, Republican Member, Rep. Greg Walden, said, "what America needs is one standard across the Internet ecosystem and the Federal Trade Commission is the best place for that standard," (Freking 2017). Furthermore, instead of focusing on one industry or set of companies, the government should create a transparent ruling that sets a standard regulation to all industries. However, there is currently a complete lack of online privacy regulation. By eliminating the original ruling, individual privacy is immediately put in danger rather than improved. Politicians must decide whether protecting companies' rights or individuals' privacies are more at stake in this Catch 22 situation.

Eliminating the Federal Communications Commission rule drastically impacts the amount of data available to advertisers. Now, "providers will be able to monitor their customers' behavior online and, without their permission, use their personal and financial information to sell highly targeted ads — making them rivals to Google and Facebook in the $83 billion online advertising market" (Fung 2017). This is big business for broadband providers and has the potential to shift the industry's core business from selling access to the Web to being the source of vast troves of consumer data. Advocates for the use of broadband data for ad targeting make a familiar claim "data-driven targeting could benefit consumers by leading to more relevant advertisements and innovative business models" (Fung 2017). In the past, AT&T had offered a discount for users who allowed the company to sell their personal data. The company claimed this was a move towards cheaper Internet, but critics claimed this was a method to charge premiums for basic privacy.

US vs. EU

The European Union serves as a realistic example of what the United States would look like with stricter data collection laws. The core difference between the E.U. and the U.S. can be summed up by opt-in vs. opt-out. In the United States, consumers must opt-out if they wish to not be tracked or have their data used. The opposite exists in the European Union. The E.U. "requires all Internet firms and any other business that processes data to obtain informed consent from the data protection authority, as well as individuals, before commencing any data collection and processing" (Chung 2014). Through this, companies cannot collect information on online users in the E.U. until a user actively opts-in. This is regulated by The European Protection Drive, an organization that sets forth principles that include, "notice, consent, proportionality, purpose limitation and retention periods" (Chung 2014). By limiting data collection on opt-in measures, E.U. citizens have more control and active understanding of data collection. Each time someone visits a new site, he is reminded data is being collected and stored on his activity, whereas in the United States there is no warning given. Data collection is an active decision in the European Union, whereas it's a passive agreement in the United States.

Self-Regulating Options

While there has been a lack of federal involvement on privacy, there are some industry enforced regulations. The FTC issued a set of four self-regulatory principles for behavioral advertising. They are, "(1) transparency and consumer control, (2) reasonable security and limited data retention for consumer data, (3) affirmative express consent for material changes to existing privacy promises, and (4) affirmative express consent to using sensitive data for behavioral targeting" (Chung 2014). Leading industry companies also formed two groups, The Online Privacy Alliance (OPA) and The Network Advertising Initiative (NAI), to implement self-

regulated guidelines and principles in regard to privacy and targeting. However, "both groups ultimately failed because of a lack of enforcement, inadequate participation from the industry and their standards offered little privacy protection" (Chung 2014).

In 2009, the American Association of Advertising Agencies, Association of National Advertisers, Council of Better Business Bureaus, Direct Marketing Association, and Interactive Advertising Bureau developed a "Self-Regulatory Principles for Online Behavioral Advertising" under the name Digital Advertising Alliance or "DAA" (The Digital Advertising Alliance 2009). The principles were created by industry professionals for self-regulation across industries. Seven main principles were: education, transparency, consumer control, data security, material changes to existing online advertising policies and practices, sensitive data, and accountability (The Digital Advertising Alliance 2009). While theses topics address main data concerns, the guidelines are very broad and lack substantial detail. The DAA has since released three additional guideline books focused on multi-site data, mobile environment, and data use across devices. However, there are no specific guidelines in direct reference to social media platforms.

Consumers can use the DAA's site to view which ad targeting and data collection companies participate in the DAA's beta WebChoices Tool, so they can take advantage of opt-out features. Users will also gain insight into how their data is being collected. Both Facebook and LinkedIn participate in these consumer-controlled services.

Future of Law

After assessing how data is collected, used, and regulated, it is clear that data is an integral part of today's society. Consumers and brands cannot deny the benefits and many positive applications of data. Since data has the possibility to harm, companies need to be held accountable. However, the laws currently protecting individual's privacy focus too much on how data is collected and not enough on how data is applied. Stronger laws should be introduced that clearly outline the boundaries to which companies can use data. As a 2016 FTC report stated:

> "The challenge for companies is not *whether* they should use big data; indeed, the reality of today's marketplace is that big data now fuels the creation of innovative products and systems that consumers and companies quickly are coming to rely upon and expect. Rather, the challenge is *how* companies can use big data in a way that benefits them and society, while minimizing legal and ethical risks" (FTC 2016).

Chapter 6: Interviews

Methods

The goal of this research was to assess social media users' understanding of privacy and personalized targeting. A total of eight in-depth interviews were conducted with adults ages 18-22 that have graduated or are currently enrolled in college. The purpose of the interviews was to gather a first-person perspective on relationships between consumer and personalized advertising. Informants were recruited through the University of Texas at Austin. For the purpose of this study, none of the informants were enrolled in the Stan Richards School of Advertising and Public Relations. Participants' majors ranged from Masters in Professional Accounting to International Relations and Global Studies. All informants were Caucasian with similar socioeconomic backgrounds. Accordingly, the generalizability of these findings to other social groups remains a question, which will be addressed by future research. To ensure privacy during data analysis, each informant was given a pseudonym. After obtaining consent from the informant, the interview was audio recorded. The audio recording was labeled by the informant's pseudonym. Once the study was complete, the audio recording was destroyed. Each interview lasted between 45 and 60 minutes.

Each interview began with a broad discussion of the informant's understanding about personalized targeting. It was designed to begin a dialogue in an open-ended manner. The interview moved gradually towards a conversation about privacy and the informant's comfort with data-driven ad targeting. Interviewees were asked to describe any memories of specific interactions with ad targeting and clearly state what kinds of personal information they would allow brands to use for targeting. If the informants felt comfortable, they were then asked to

show their online behaviors and interests, as defined by Facebook's Ad Preferences. All informants participated. The interviews were held in a conversational style, where the informant largely determined the trajectory of the interview dialogue. Prompts were used when necessary to further understand the meaning of their experiences. Informants were asked to elaborate on various statements and provide more explanation after discussing specific experiences. All informants were questioned whether they had AdBlocker installed on their browser. AdBlock is a free Google Chrome extension that blocks banners, pop-ups, tracking, malware, and more.

Results

The purpose of this research was to explore social media users' understanding of ad targeting and privacy policies. The analysis revealed disconnect between what information is currently being used by brands and what users are comfortable with. Findings also showed that informants felt a lack of control about how their online behavior was used. These findings are expounded below through individual summaries and general trends.

Individual Analysis

Michelle

Michelle is a 21-year-old student majoring in International Relations and Global Studies. She spends roughly two hours daily on Instagram, Facebook, Snapchat, and LinkedIn. She has had AdBlock installed through Google Chrome for the past year.

At the beginning of the interview, Michelle said she was fine with brands using personalized targeting. However, as the interview progressed she described actions associated with personalized targeting as "kind of annoying." In regards to Facebook, she thinks, "they use

everything" since the platform has access to information that is normally private to the public. While her tone was reluctant towards ad targeting, she believed "we are the generation that understands we can't have privacy because of social media [...] so we are okay with companies using our information [...] because we are familiar with that idea." Michelle expressed concern over ad targeting, but also displayed confidence that she was part of a generation that understands the complexity of privacy and convenience.

Kristen

Kristen is a 21-year-old student in The McCombs School of Business, majoring in Management. She spends roughly two hours daily on Instagram, Facebook, Snapchat, Pinterest, LinkedIn, and Twitter. Kristen does not use AdBlock.

Kristen was initially the least worried about personalized targeting. She was practical about the necessities of advertising for business; however, she was unaware of the full scope of data sharing. When asked about her comfort level with Facebook sharing her data, Kristen said, "personally, I don't really care. For me, I have nothing to hide so, if I'm putting it on Facebook [...] I'm giving them permission." While Kristen was comfortable with Facebook sharing her information, she had a false understanding of how data was shared. For Kristen, she believed, "what [information] is on Facebook stays on Facebook". In reality, shared data can be used beyond Facebook's owned platforms.

Out of all the interviewees, Kristen was ironically the most uncomfortable when shown her Facebook Ad Preferences. According to Facebook, there were 120 companies who had her contact information. This was in addition to the 144 companies whose websites or apps she had

used through Facebook. Her initial reaction was, “Wow, I need to be more careful [...] I don’t even know a lot of these [companies] [...] why is this happening to me?” Even though she was shocked by the amount of companies with her information, she still attributed the fault to herself. She said, “Facebook isn’t being deceiving [...] if you read the fine print you will know this about [Facebook] [...] kind of the customers fault for not reading the terms.” As a business student, Kristen kept commenting on how this was a smart business move by brands. She was seemingly less concerned about her own privacy than she did about operating a profitable business. During the interview, Kristen acknowledged that her business classes had spoken briefly on big data and privacy, but the majority of her knowledge came from general discussions with friends and popular media.

Anastasia

Anastasia is a 22-year-old student majoring in Youth and Community Studies. She does not use AdBlock. Currently, Anastasia is active on Facebook, Instagram, Snapchat, and Pinterest for roughly two hours a day. She spends the most time on Facebook and Instagram.

From the start of the interview, Anastasia made it clear that she found personalized targeting “threatening” and “an invasion of privacy” because, “it takes information I haven’t knowingly given permission to access.” While Anastasia was concerned about her privacy, she said it did make shopping online “convenient;” she clearly understood the costs associated with the benefits. Anastasia further mentioned she was an avid online shopper, so re-targeting was a practice she witnessed frequently.

Anastasia said the primary forms of targeting she noticed online were ads directly related to her online shopping. She humorously mentioned she sometimes gets targeted for breast milk, formulas, and breast pumps. While Anastasia disclosed she is not pregnant or a mother, she babysits frequently, has a six-month old niece, reads mom blogs, and follows baby Instagrams. Therefore, she understands why she is being targeted and finds the ads entertaining, but also "kind of presumptuous".

Patricia

Patricia is a 21-year-old student getting her Masters of Professional Accounting. She occasionally uses AdBlock and is active on Facebook, Instagram, Snapchat, and LinkedIn. She spends around an hour daily on social media. Patricia was one of the more knowledgeable interviewees on this topic from taking a Management Information Systems (MIS) class in school. She said the big takeaway from the class is that Big Data is where the future is and students who get into Big Data are guaranteed a profitable job.

Her initial opinion was, "from a business major perspective, I get why it's done" She said, "to some extent I agree, but some extent I think it's too much". From a personal standpoint she said personalized targeting makes her a "little uncomfortable because it means they're searching through my history of what I'm doing [...] they have access to my information [...] I question how much they know". While Patricia admits to not reading privacy policies, her coursework taught that users "only have to read one clause with specific words in bold […] if [users] don't see [important clauses] highlighted in the paragraph [the company is] liable". This might be one reason why Patricia feels comfortable staying active on social media, even with personal privacy concerns.

Emily

Emily is a 22-year-old student majoring in Plan II Honors and receiving her Masters in Professional Accounting. She does not use AdBlock and is active on Facebook, Instagram, and LinkedIn. She was the only interviewee who does not use Snapchat. Emily claims to use social media less than an hour a day.

Emily believes personalized targeting is "freaky" and "weird". For Emily it was "freaky" how quickly her online behaviors turned into personalized advertising. She said, "it's weird how fast I could be looking at something and [then] it pops up on my advertisements [...] in the same day. [It's] crazy how instantaneous [personalized advertising] is". She also recognized cross-device advertising, noting how an action on her computer would translate into an advertisement on her phone. She said she gets targeted on Instagram for different fitness studios. Emily attributes this to her front-desk job at a local cycling studio. Compared to other interviewees, Emily was more perceptive and aware of ads being served to her. Although there were limitations to her knowledge, Emily made logical guesses about how her data was being used.

Kelly

Kelly is a 22-year-old student majoring in Government with the Business Foundations Certificate. Kelly spends one to two hours a day looking at Facebook, Instagram, Snapchat, LinkedIn, Pinterest, and Google Chat. She does not use AdBlock.

Kelly's opinion on personalized targeting was complex. While she found it to be "really creepy" and "almost too targeted," yet admitted, "I like some of the items they suggest". Specifically, it angered her that brands do not use subtlety in their targeting. She preferred social platforms to

show similar items to her search history, rather than the exact item she looked at online earlier that afternoon. For example, she wished Nordstrom showed an ad for running shoes, rather than the exact pair of Nike sneaker's she had recently viewed online. When looking through her Facebook Ad Preferences, Kelly saw a list of apps with her information. She said some of the apps were "weird" since she could not recall whether she logged in through Facebook or not. Kelly also looked at her information and found most of Facebook's inferences correct. Facebook correctly identified her as an "Event Creator" since she is the type of person to host an event. The platform also correctly identified she lived in a "house-mate based household". Kelly found this piece of information odd, since she could not logically deduce how Facebook predicted she lived with a roommate.

Lauren

Lauren is a 21-year-old student majoring in Business, Consulting, and Change Management through The McCombs School of Business. She uses Facebook, Snapchat, Instagram, and LinkedIn for at least an hour and a half each day. Lauren currently has AdBlock installed.

Lauren repeatedly conveyed her distaste for all forms of advertising, stating, "I prefer no ads. I've never clicked on ads [...] I ignore them [...] I have always been that way". While Lauren believed she never acted on advertisements, her Facebook Ad Preferences disclosed that she had actually clicked on 45 different ads. When looking through the specific ads she clicked, she stated that she did not realize that more than half of them were advertisements. This demonstrated a potential lack of awareness of what advertisements look like in 2017. As brands shift towards native advertising, advertisements blend in with other posts and the line between advertising and content is blurred.

Lauren was the only interviewee to express concerns about medical related, data collected. She said, "I don't think anything medical belongs on the Internet. [Medical information] belongs between a patient and their physician or anyone who is taking care of them". At the end of the interview, Lauren saw that "dermatology" was one of her interests according to Facebook. A few years ago Lauren said she was on Accutane, but that was information she did not want Facebook to know.

Monica

Monica was the last respondent of this study. She was a 22 year old majoring in International Relations and Global Studies. She has AdBlock downloaded on her computer to block pop-ups when she streams movies. Currently, Monica uses Facebook, Instagram, Snapchat, LinkedIn, and Twitter for roughly two hours per day.

Overall, Monica appreciated targeted ads and did not want to alter the type of ads served to her. While she mentioned she did not shop online regularly, she enjoyed seeing clothing she might be interested in trying on in person. Monica also believed that Facebook made inferences about her based on her online behavior and her networks. When asked how Facebook made these inferences, Monica replied, "[Facebook] tracks all these pages and [the] type of information [...] viewed by me, my networks, and our mutual connections. [And if] there's a general trend, they're able to find it".

When looking through her Facebook Ad Preferences, Monica said her identification was "pretty accurate". She explained, "[My interests according to Facebook] can be pretty broad, but also

pretty specific [...] it's a fine way to categorize me as a user [...] nothing I would be ashamed of if I posted [my Ad Preferences] publically".

Common Themes

Law

A main goal of the interviews was to explore what individuals know about privacy legislation. At the time of the study, the United States was undergoing a shift in politics from a Democratic White House under the Obama administration to a Republican White House under the Trump administration. Accordingly, there was plenty of public debate regarding the role of government in regulating online privacy. Even with the influx of media coverage, the majority of respondents were either unaware or misinformed about the lack of U.S. regulations.

When asked whether user information is primarily protected from a platform's privacy policy or United States law, most interviewees believed it was the law. Monica's reasoning was, "if platforms could be more public they would [...] I think there are regulations that are given to [platforms] by government law." In reality, social platforms have immense control over how they use their member's data. When questioned about their awareness of specific regulation, Monica replied, "I think I've heard of [a specific regulation] before I just can't recall any specific legislation. I don't think platforms would [maintain user's privacy] on their own. I think [platforms] need some regulations to ensure everyone's information stays protected and private." Monica's answer highlights why there is a need for regulation. Selling user-data makes platforms profitable, so there is little incentive for these businesses to refrain from exchanging user data. Although platforms must maintain trust with their users, the interviews clearly demonstrated that

users were quite frankly too lazy to track how their data was being used. Monica's response also exemplified a common theme throughout all respondents; they believed there is proper regulation regarding user data in the United States, but are uneducated and informed about specific details.

When asked about privacy regulation, Kelly, a government major, said, "I think the government needs to do anything they need to keep you safe." She had familiarity with two privacy related regulations, the first being The Patriot Act. She described The Patriot Act as legislation that allows government to "spy on you so they can protect you [by] scanning emails and wiretapping." As for the second regulation, Kelly was unclear and vague. She described it as, "that law that was recently repealed or enacted that they can sell your information." Her broad description demonstrated an awareness of legislation but ignorance towards its implications. This was significant because this act is more likely to impact Americans everyday than the Patriot Act. Speaking with Lauren, she was slightly more informed and noted that the Net Neutrality Act did not pass. As for the impacts of this action, Lauren said, "I'm sure there is other [legislation] in place [protecting privacy], but [there are] discrepancies in interpretation because Internet and Big Data are so new." Lauren correctly pinpointed an obstacle with Big Data legislation. As discussed previously, discrepancies between how Personally Identifiable Information (PII) is defined alters whether certain actions are legal. Although Lauren correctly predicted a main issue in U.S. privacy legislation, she did not appear concerned or passionate about improving privacy legislation.

There were also a few respondents who recognized legislation was not as strict as they might hope. Patricia made an interesting comparison between Big Data and the Enron scandal. She

said, “I believe government creates laws after problems occur. After a problem happens, then laws will be created to prevent it from happening again [...] or at least to the same degree. [It’s] like Enron, auditors became a mandatory part of any public company’s process”. While Patricia's comparison is extreme, there is a degree of validity in the statement. Three main factors in the 2000’s Enron scandal were a lack of regulation, insufficient public knowledge, and the absence of transparency. The same concerns can be said about Big Data, and like the energy market, Big Data is an enormous industry. One research firm even predicts sales of Big Data and analytics tools will reach $203 billion by 2020 (IDC 2016). Improper use of user data could lead to widespread problems across a series of industries.

Another common sentiment was that government could not keep up with advancements in technology. When asked if there were laws on protecting user data, Emily said, “I imagine what we have is insufficient. Our policy makers can’t keep up with [technology] and it’s constantly evolving.” Michelle also believed our government is, “still pretty far behind” and our legislation had a lot of “grey area.” After thinking about what she said, Michelle added her concern of what would happen if someone hacked into a data broker’s database.

The most practical response about the government’s role in protecting users’ privacy came during Emily’s interview. When Emily was asked whether the responsibility of protecting a user’s privacy should fall on the platform or the government, she said, “I think it is kind of more than a yes or no answer. Overall the responsibility is on the lawmakers, but the platforms have a moral responsibility on how they handle the information. [Platforms] need to be hyper-aware and respectful of what they’re doing; lawmakers need to be there to regulate it all.” Emily’s argument was that platforms should be responsible for making moral decisions, but government regulation

also needs to be present to monitor any platform that behaves unethically. Even if nine out of ten platforms treat user data correctly, that one bad platform could cause major damage in the United States.

Geo-Targeting

One of the most shocking results of the interviews was discovering widespread disapproval of geo-targeting. When interviewees were asked if they were comfortable with social platforms collecting and sharing data based on their location, all said no. The interviewees were then asked to specifically define their comfort with different levels of location targeting. The study found that all respondents were comfortable with companies knowing they were in the United States, but when the location got more specific (i.e. the south, Texas, Austin, Zip Code, and finally current location), fewer interviewees approved. Interviewees did not want companies knowing their current location because, as Monica articulated, "I think [sharing my current location] is too much supervision and invasion of personal space. I don't want [companies] to track my every movement [...] they can know my general location." Patricia agreed that she did not want her exact location known, "unless [she] physically checks in [and is] sharing [her location] with everyone". However, she disclosed that she never checks in and believes anyone who shares his or her current location is an "idiot". Although geo-targeting is a prevalent tool that is used by both small companies and large corporations, the interviewees in this study were unaware and unsupportive.

Data-Sharing

As discussed earlier, data sharing poses the greatest risk of violating user information. However, a reasonable hypothesis suggests that an average Internet user is unfamiliar with data brokers and how their data is shared. This argument was supported by the interviews in this study. Although respondents were aware social platforms collected data on them, most believed this data was kept within the company. For example, Kelly believed that Facebook, "shares [her information] with Instagram but not with any other companies." Likewise, Kristen said it was, "nice to know what [information] is on Facebook stays on Facebook." When told their information was shared outside of the social platforms, Emily said, "I don't like that my information could get to third parties at all [...] I don't even like that my email can get to them because email is tied to so much to what I do".

Out of the eight respondents, six respondents believed their data stayed within Facebook's jurisdiction. The other two respondents, Lauren and Patricia, knew Facebook profited off selling user data. It is worth noting that Lauren and Patricia were introduced to the business benefits of Big Data through a required business course, Management Information Systems (MIS). During Lauren's interview, she was asked whom social platforms share user data with. Lauren replied, "anyone who is willing to pay for it [Facebook is] willing to share it." During Patricia's interview, she was asked what social platforms do with user data. She replied, "[social platforms] sell [user data] to companies [because] that's what Big Data is [and] that's where the money is." As business students, both understood the advantages of brands buying user data. Still, Lauren voiced her opposition towards Facebook sharing her data. Her reasoning was," if I wanted to share it with some other entity with Facebook, I would."

Anonymous

During the interviews, respondents were asked how anonymity impacted their comfort with data sharing. Michelle voiced a common opinion stating, "if it's anonymous it doesn't matter." Meaning, she was comfortable with her data being shared as long as it was anonymous. Michelle commented, "we are the generation that understand we can't have privacy because of social media, so we are okay with companies using our information."

Emily shared that she does not "mind being put into clump of type of people, but a lot of [Facebook inferences indicate a] specific person". She said, "all stuff figures out who I am, not just the type of person, but me, specifically who I am". Emily expressed fear in Facebook's ability to infer and pinpoint specific details about her life.

Control

Another main theme to come out of the study was an overall sentiment that platform users lacked any control over their data. Instead of feeling motivated to alter the status quo, interviewees made statements of complacency. For example, when asked if she would like more restrictions on data usage, Lauren replied, "no, I really feel like what's out there is out there [...] it's almost too late." Although Lauren had major issues with interest based targeting, she believed there was nothing she could do to stop it. Kelly shared the same sentiment. When asked if she was okay with Facebook profiting off inferences they made about her she said, "no. I mean it's not like I'm okay with [Facebook profiting off inferences about me] but what can you do about it?" Similarly, Lauren said, "I think even if a company gives me the option to limit data, they would still be collecting data." When asked how that made her feel, she said, "Not angry, a little paranoid, [...] I feel like a paranoid person in this interview."

One way the interviewees appeared to maintain some power is by controlling how they behave online. Monica said she was taught that a "user needs to use discretion because once [she] puts information [she doesn't] know where it goes." By managing what photos are posted or what pages are liked, users can limit the amount of data platforms collect on them. However, for information that is posted online, Monica believes "platforms should respect the wishes of users when they want to be private".

Another interesting way interviewees kept control over their information were through private accounts. The females interviewed displayed confidence that their private accounts made them smart users of social media. Seven interviewees had a private Instagram profile, all claimed their Facebook profile was fairly private, and all interviewee's on Snapchat only accepted close friends as Snapchat friends. While having a private account protects a user's posts from being shared with strangers, it does not stop the social platforms from collecting and sharing their data. Most users have a false understanding of private accounts in which they believe they have full control over who sees their online activity. One interviewee, Michelle, understood this. Speaking about Instagram, she said, "[users] are controlling who sees [their posts], but not controlling what Instagram sees". Users should be equally concerned about what photos a stranger can view and what information a platform can collect.

While most interviewees tried to keep the maximum amount of control, Kristen was comfortable losing some power because, "ultimately it's all just entertainment". However, social platforms are equal parts entertainment and big business. While social platforms give entertainment for users, platforms function and profit off being a source of data-collection. What Kristen does not

understand is that her online behavior, even if it's just for entertainment, says a lot about who she is. Brands purchase this information and make inferences about her as a consumer. This impacts what types of messaging, products, or services she receives daily. While a targeted ad for shoes does not significantly impact Kristen's life, being served specialized political ads for a certain party or politician can influence how she votes or behaves offline.

Trust

Although respondents were weary of their data being shared, there was an overall sentiment of trust in the different social media platforms. . Even if the respondent didn't trust advertisers and data brokers, they trusted the leaders of Facebook, Instagram, Snapchat, and LinkedIn. One respondent, Kelly, was asked to rank her trust in Facebook one out of ten. She answered saying, "I would give them a 6.5 [...] I think Mark Zuckerberg has a pretty strong brand that filters down to the company." When asked what makes her think that she said, ""[Zuckerberg is] kinda outspoken about important causes and he is pretty philanthropic and he just seems like a pretty good person." Here, Kelly attributes her trust in Facebook directly to its founder. While Zuckerberg definitely has impact on Facebook's operations, he is only one executive in a multi-billion dollar company. Respondents should understand that Facebook is not a small run start-up, rather a major company. The social platform is America's third most valuable company and oversees more than six different companies. Therefore, trust in Facebook should be assessed by the company's explicit business policies rather than its founder's ethics.

Convenience

Although interviewees were concerned about their privacy, most found targeted ads helpful. Emily provided a specific example that proved targeted ads assisted in her buying process. She had recently shopped online for natural skincare products. Emily recalled she "got an ad on Instagram for another natural skincare [she] hadn't heard of before. [Emily] was intrigued by the product because it was on [her] mind." Although Emily felt weird about being targeted, she appreciated the opportunity to learn about a relevant brand. Even with privacy concerns, Emily admitted she would still continue using the sites "because [her] pros and reasons for using the sites still outweigh how much [data sharing] bothers [her]." She uses social platforms for "both a utility and enjoyment".

One respondent, Lauren, was the outlier in the group and would prefer to never receive targeted ads. She said, "I don't care about ads, so the less ads I have, the better. The less information [companies] have on me the better [...] I would rather have less targeted ads than targeted ads but I can see the appeal of some people". Lauren's opinion demonstrates that all consumers are not the same. While some individuals find targeted ads helpful, some are greatly turned off by their existence. Brands should recognize this reality and limit their ads to these individuals.

Areas of Discipline

An interviewee's area of study had a surprising impact on her responses. On average, business students applauded companies who utilized targeting in their advertising campaigns. While they were not personally comfortable with their information being shared, they agreed it was a business practice they would participate in as an employee. Students majoring in government and international relations, on average, believed the government had more regulations in place to

protect its citizens. For future research, it would be interesting to interview students studying computer science, engineering, or health related majors. These students might provide an alternative perspective on software, data technologies, and health records.

Future Recommendations

This study exposed several areas for future research. Since this study was limited to female college students, it would be interesting to compare these results to responses by male students and people of older generations. A more comprehensive study would include participants of varying socioeconomic backgrounds and education levels. While not publically available, it would be fascinating to see how many Facebook users have viewed their Facebook Ad Preferences, and the frequency of views. Does viewing Facebook Ad Preferences change behavior, or is it mainly a tool for public awareness?

Chapter 7: Conclusions

The initial goal of this thesis was to examine the ethical boundaries of ad targeting on social media. Through research, it became apparent that there was a larger discussion to be had. As covered in my thesis, social platforms do not operate in isolation. Social media platforms are only one part of a larger media ecosystem that survives off the transfer and usage of user data. While social platforms have created privacy policies to address transparency and privacy concerns, their policies are at often vague and can easily be corrupted through loopholes. Data has largely transformed the advertising industry and how brands communicate with consumers. While behavioral targeting increases ad relevancy, it utilizes private information to do so. Brands must be aware and conscientious regarding how they apply data sets to different marketing campaigns.

My thesis also discovered a general lack of public awareness for how companies share user information. Individuals expressed general concern for their privacy, but lacked knowledge on how their data was being regulated. Overall, individuals had a misperception that more government regulation and enforcement currently existed. Interviewees demonstrated that even with Facebook's attempt at greater transparency through Facebook Ad Preferences, most users were unaware of its existence and their own opportunities to increase control.

Moving forward, stricter and more explicit laws should be adopted by the U.S. government. These laws should focus less on how data is collected and more on how data can be used. It is futile to try and limit the amount of data collected, therefore efforts should be focused on protecting user data from being abused.

While my thesis focused on social media, similar findings could be applied to data collection regarding new technologies such as wearables and AI systems. With wearables, companies track a user's heart rate and physical activity. There should be strict laws on how brands can use this data to sell products or services *before* it becomes a problem. Each and every day, there is more data being collected, sold, and interpreted. In sum, data is powerful and an integral part of today's marketplace. Knowing this, it is imperative we keep lobbying for stronger data laws and pushing towards greater public awareness. Currently, consumers only understand how a portion of their data is used; it is time they see the full picture.

Bibliography

Aaker, Jennifer A. "Nontarget Markets and Viewer Distinctiveness: The Impact of Target Marketing on Advertising Attitudes." *Journal of Consumer Psychology*, vol. 9, no. 3, pp. 127-40, doi:10.1207/S15327663JCP0903_1. Accessed 6 Nov. 2016.

"Advertising Policies." *Facebook*, 5 May 2016, www.facebook.com/policies/ads/. Accessed 6 Nov. 2016.

Angwin, Julia, and Terry Parris, Jr. "Facebook Lets Advertisers Exclude Users by Race." *ProPublica*, 28 Oct. 2016, Facebook Lets Advertisers Exclude Users by Race. Accessed 1 Nov. 2016.

Blake, Katy Elle. "The 2016 LinkedIn Stats You Should Know - Updated!" *LinkedIn*, 17 Aug. 2016, www.linkedin.com/pulse/2016-linkedin-stats-you-should-know-updated-katy-elle-blake. Accessed 2 Apr. 2017.

Business Insider. 23 Jan. 2017, www.businessinsider.com/snapchat-is-opening-itself-up-to-more-ad-targeting-2017-1. Accessed 28 Jan. 2017.

Chung, Yuen Yi. "Goodbye PII: Contextual Regulations for Online Behavioral Targeting." *Journal of High Technology Law*, vol. 14, no. 2, 2014, pp. 413-50.

"Company Info." *Facebook*, 5 May 2017, newsroom.fb.com/company-info/. Accessed 7 May 2017.

"Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy." *Obama White House*, Feb. 2012, obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf. Accessed 6 Mar. 2017.

"Custom Audiences Terms." *Facebook*, 30 Sept. 2016, www.facebook.com/ads/manage/customaudiences/tos.php?_=_. Accessed 6 Nov. 2016.

Data Brokers: A Call for Transparency and Accountability. 2014, www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf. Accessed 28 Jan. 2017.

"Distribution of Snapchat Users in the United States as of February 2016, by Age." *Statista*, Feb. 2016, www.statista.com/statistics/326452/snapchat-age-group-usa/. Accessed 13 Feb. 2017.

Freking, Kevin. "Republicans Just Voted to Allow Internet Companies to Sell Your Browsing History." *Time Inc. TIME*, time.com/4716033/house-internet-browsing-history-fcc-comcast-verizon/?xid=time_socialflow_facebook. Accessed 29 Mar. 2017.

Fung, Brian. "The FCC Just Passed Sweeping New Rules to Protect Your Online Privacy." *The Washington Post*, 27 Oct. 2016, www.washingtonpost.com/news/the-switch/wp/2016/10/27/the-fcc-just-passed-sweeping-new-rules-to-protect-your-online-privacy/?utm_term=.1f6ba4bf1dc7. Accessed 29 Mar. 2017.

---. "The House Just Voted to Wipe Away the FCC's Landmark Internet Privacy Protections." *The Washington Post*. *Washington Post*, www.washingtonpost.com/news/the-switch/wp/2017/03/28/the-house-just-voted-to-wipe-out-the-fccs-landmark-internet-privacy-protections/?utm_term=.7d526f37d72d.

Ha, Anthony. "Gap Campaign Rethinks Old-School Bus Station Ads." *Tech Crunch*, 11 Mar. 2012, techcrunch.com/2012/03/11/gap-geofence-campaign/. Accessed 25 Nov. 2016.

Handley, Lucy. "Paid Media Spend on Social up by 65 Percent, Instagram Leads Growth: Report." *CNBC*, 12 Jan. 2017, www.cnbc.com/2017/01/12/paid-media-spend-on-social-up-by-65-percent-instagram-leads-growth-report.html. Accessed 3 May 2017.

Heath, Alex. "Snapchat Is Opening Itself up to Advertisers of All Sizes with New Buying Tools." *Business Insider*, 4 May 2017, www.businessinsider.com/snapchat-announces-self-service-ad-tools-for-small-businesses-2017-5. Accessed 4 May 2017.

Helmore, Edward. "Snapchat Shares Soar 44% to Value Loss-making Company at $28bn." *The Guardian*, 2 Mar. 2017, www.theguardian.com/technology/2017/mar/02/snapchat-ipo-valuation-evan-spiegel-bobby-murphy-snap-inc. Accessed 2 May 2017.

Hill, Kashmir. "How Target Figured out a Teen Girl Was Pregnant before Her Father Did." *Forbes*, 16 Feb. 2012, www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#7d19ca2b34c6. Accessed 6 Nov. 2016.

Ingis, Stuart P., et al., editors. *Self-Regulatory Principles for Online Behavioral Advertising*. July 2009, www.aboutads.info/resource/download/seven-principles-07-01-09.pdf. Accessed 1 May 2017.

Iyer, Ganesh, et al. "The Targeting of Advertising." *Marketing Science*, vol. 24, no. 3, Summer 2005, pp. 461-76. *JSTOR*, www.jstor.org/stable/40056974.

Joseph, Seb. "Snapchat is opening up its ad platform ahead of its planned IPO." *Business Insider*, 31 Jan. 2017, www.businessinsider.com/snapchat-opens-up-ad-platform-ahead-of-its-planned-ipo-2017-1. Accessed 1 Feb. 2017.

Kerr, Gayle. "Does Traditional Advertising Theory Apply to the Digital World?" *Journal of Advertising Research*, June 2015, thearf-org-aux-assets.s3.amazonaws.com/jar/Kerr.pdf. Accessed 6 Nov. 2016.

Kessler, Sarah. "The History of Advertising on Facebook." *Mashable*, 28 June 2011, mashable.com/2011/06/28/facebook-advertising-infographic/#JOTS4AKGCSqy. Accessed 1 May 2017.

Kruikemeier, Sanne, et al. "Political Microtargeting: Relationship between Personalized Advertising on Facebook and Voters' Responses." *Cyberpsychology, Behavior, and Social Networking*, vol. 19, no. 6, June 2016, doi:10.1089/cyber.2015.0652.

MacDonal, Aleecia. "Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising." *TPRC*, papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092. Accessed 6 Nov. 2016.

Madden, Mary. "Public Perceptions of Privacy and Security in the Post-Snowden Era." *Pew Research Center*, 12 Nov. 2014, www.pewinternet.org/2014/11/12/public-privacy-perceptions/. Accessed 13 Feb. 2017.

Martinez, Christian. "Driving Relevance and Inclusion with Multicultural Marketing." *Facebook*, 28 Oct. 2016, newsroom.fb.com/news/h/driving-relevance-and-inclusion-with-multicultural-marketing/. Accessed 6 Nov. 2016.

Mayer-Schönberger, Viktor. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt, 2013.

Merrill, Jeremy B. "Liberal, Moderate or Conservative? See How Facebook Labels You." *The New York Times*, 23 Aug. 2016, Liberal, Moderate or Conservative? See How Facebook Labels You. Accessed 3 Nov. 2016.

O'Reilly, Lara. "Snapchat Is Finally Learning to Love the 'Creepy' Advertising It Once Said It Hated." *Business Insider*, 3 Dec. 2015, www.businessinsider.com/snapchat-advertising-measurement-targeting-2015-12. Accessed 6 Feb. 2017.

Pew Research Center. "Percentage of U.S. Internet Users Who Use Linkedin as of April 2016, by Age Group." Statista - The Statistics Portal, Statista, www.statista.com/statistics/246172/share-of-us-internet-users-who-use-linkedin-by-age-group/, Accessed 2 Apr 2017

"Press Release." *IDC*, 3 Oct. 2017, www.idc.com/getdoc.jsp?containerId=prUS41826116. Accessed 14 Apr. 2017.

Rath, Julien. "Data Shows Nearly Half of Snapchat's Revenue Comes from Discover Ads." *Business Insider*, 31 Jan. 2017, www.businessinsider.com/data-shows-nearly-half-of-snapchats-revenue-comes-from-discover-ads-2017-1. Accessed 13 Feb. 2017.

"S. 913 — 112th Congress: Do-Not-Track Online Act of 2011." www.GovTrack.us. 2011. March 6, 2017 <https://www.govtrack.us/congress/bills/112/s913>

Schlee, Christian. *Targeted Advertising Technologies in the ICT Space: A Use Case Driven Analysis*. Wiesbaden, Springer Vieweg, 2013.

"Self-Regulatory Principles for Online Behavioral Advertising." *Interactive Advertising Bureau*, July 2009, www.iab.com/wp-content/uploads/2015/05/ven-principles-07-01-09.pdf. Accessed 6 Nov. 2016.

Sloane, Garrett. "Facebook Pushes Back against Report of Housing Ads Targeted by Race." *Ad Age*, 28 Oct. 2016, adage.com/article/digital/facebook-ads-target-exclude-groups-race/306531/. Accessed 6 Nov. 2016. This article responds to a ProPublica article regarding Facebook advertiser's ability to target ethnicities. It claims that Facebook does not in fact allow the discrimination of race on its site.

---. "Facebook Tests Letting People Block Alcohol or Parenting Ads to Avoid Stirring Painful Memories." *Ad Age*, 16 Dec. 2016, adage.com/article/digital/facebook-lets-users-block-ads-stir-painful-memories/307193/. Accessed 21 Apr. 2017.

---. "How Snapchat's CEO Plans to Conquer the Advertising World." *Adweek*, 14 June 2015, www.adweek.com/news/technology/heres-how-snapchats-ceo-plans-conquer-advertising-world-165339. Accessed 28 Jan. 2017.

---. "Snapchat's New Targeting Tools Could Help Improve Ad Results." *Ad Age*, 28 Dec. 2016, adage.com/article/digital/snapchat-s-targeting-tools-improve-ad-results/307307/. Accessed 28 Jan. 2017.

Smith, N. Craig, and Elizabeth Cooper-Martin. "Ethics and Target Marketing: The Role of Product Harm and Consumer Vulnerability." *Journal of Marketing*, vol. 61, no. 3, July 1997, pp. 1-20, doi:10.2307/1251786. Accessed 6 Nov. 2016.

"Snapchat Pushes Further into Digital Ad Targeting." *Wall Street Journal*, edited by Mike Shields, 13 Sept. 2016, www.wsj.com/articles/snapchat-pushes-further-into-digital-ad-targeting-1473778896. Accessed 28 Jan. 2017.

"Snap Inc. Advertising Policies." *Snap Inc.*, www.snap.com/en-US/ad-policies/. Accessed 28 Jan. 2017.

Terlep, Sharon. "P&G to Scale Back Targeted Facebook Ads." *The Wall Street Journal*, 17 Aug. 2016. *Wall Street Journal*, www.wsj.com/articles/p-g-to-scale-back-targeted-facebook-ads-1470760949. Accessed 6 Nov. 2016.

Wall Street Journal. 19 Jan. 2017, www.wsj.com/articles/snapchat-to-enable-ad-targeting-using-third-party-data-1484823600. Accessed 28 Jan. 2017.

Author Biography

Nicole Lang is a native Texan. At the University of Texas at Austin, she studied Plan II Honors in The College of Liberal Arts, alongside her pursuit of an Advertising degree from The Moody School of Communications, where she was also enrolled in the TexasMedia Program. During her time in college, Nicole served as Vice President of Philanthropy for the Omega Chapter of Alpha Epsilon Phi. Her junior year, she had the wonderful opportunity to study abroad in London, England. Drawing on her love for advertising and social media, Nicole will begin work as a Paid Social Associate for GroupM in New York City. Nicole will work with Target Corporation through GroupM's Team Arrow Partners. She plans to take her knowledge of data, privacy, and targeting and make smart and strategic decisions in the future.